НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
Факультет інформатики та обчислювальної техніки
Кафедра автоматики та управління в технічних системах

«До захисту допущено»
Завідувач кафедри
_____ О.І. Ролік
«___»_____2019 р.

Дипломний проект

на здобуття ступеня бакалавра
з напряму підготовки 6. 050201 «Системна інженерія»
на тему: «Система захисту інформації в корпоративній мережі»

Виконав:
студент IV курсу, групи ІА-51
Галай Ярослав Олександрович _____
Керівник:
Професор кафедри АУТС, д.т.н. доцент Корнієнко Б. Я.
_____
Рецензент:
к.т.н., доцент ОТ, Павлов В. Г.
_____

Засвідчую, що у цьому дипломному проекті немає запозичень з праць інших авторів без відповідних посилань.
Студент _____

Київ – 2019 рік

Пояснювальна записка
до дипломного проекту
на тему: «Система захисту інформації в корпоративній мережі»

Київ – 2019 рік

АНОТАЦІЯ

Структура та обсяг роботи. Пояснювальна записка дипломного проекту складається з трьох розділів, містить 38 рисунків та 14 джерел.

Дипломний проект присвячений вирішенню проблеми захисту в корпоративних мережах.

Метою роботи є винайдення системи заходів, які реалізовані програмно та можуть бути швидко розгорнуті на сервері або комп'ютері з операційною системою Windows/Linux/MacOS. Система заходів вирішує проблему захисту інформації за допомогою електронно-цифрового підпису та брандмауера в середині програмної реалізації.

У розділі постановка задачі описуються критерії розроблюваної системи захисту.

У розділі огляд предметної області та існуючих рішень розглядається проблема компрометації корпоративних серверів та інформації, а також оглядаються існуючі рішення для вирішення даних проблем.

У розділі обґрунтування вибору та реалізація наводиться обгрунтування вибраного рішення та описується програмна реалізація. Результати тестування наведені наприкінці даного розділу.

АННОТАЦИЯ

Структура и объем работы. Пояснительная записка дипломного проекта состоит из трех разделов, содержит 38 рисунков и 14 источников.

Дипломный проект посвящен решению проблемы защиты в корпоративных сетях.

Целью работы является изобретение системы мероприятий, реализуемых программно и могут быть быстро развернуты на сервере или компьютере с операционной системой Windows / Linux / MacOS. Система мероприятий решает проблему защиты информации с помощью электронно-цифровой подписи и брандмауэра в середине программной реализации.

В разделе постановка задачи описываются критерии разрабатываемой системы защиты.

В разделе обзор предметной области и существующих решений рассматривается проблема компрометации корпоративных серверов и информации, а также осматриваются существующие решения для решения данных проблем.

В разделе обоснования выбора и реализация приводится обоснование выбранного решения и описывается программная реализация. Результаты тестирования приведены в конце данного раздела.

ABSTRACT

Structure and scope of work. The thesis consists of three sections, containing 38 figures and 14 sources.

The diploma project is devoted to solving the problem of protection in corporate networks.

The thesis is devoted to development the system of mechanisms that are implemented programmatically and can be quickly deployed on a server or computer running the Windows / Linux / MacOS operating system. The system of mechanisms solves the problem of information security with an electronic digital signature and a firewall in the software implementation.

In the section of setting the task describes the criteria of the developed system of protection.

In the topic overview and existing solutions, the problem of compromising corporate servers and information is discussed, as well as existing solutions to address these issues are reviewed.

In the justification section of the selection and implementation, the justification of the chosen solution is given and the program implementation is described. Test results are given at the end of this section.

ВСТУП

Корпоративні мережі в сьогоденні займають значну частину інфраструктури компаній як IT – напрямку так і компаній інших виробничих чи сервісних галузей. Не можливо уявити компанію без найменшої, хоча б локальної, мережі. Сполучення робочих станцій та серверів у мережу обміну інформацією дозволяє синхронізувати працю декількох людей, офісів, компаній та навіть країн. Переоцінити вплив корпоративних мереж дуже важко.

Але під час передачі, зберігання, обчислення, тощо, інформації виробничі компанії стикаються з проблемою, яка присутня завжди, якщо в локальній чи глобальній мережі присутній обмін інформацією між станціями, мережевими сегментами або власне мережами. Проблема захисту інформації в корпоративних мережах стоїть дуже гостро, тому що в сучасному світі порушення безпеки інформації може призвести до серйозних наслідків та мільйонних збитків для корпорацій. Так пошкодження інформації при передачі між мережами чи її сегментами може призвести до фатальних наслідків, якщо це виміри від яких залежить точність подальших обчислень. Затримка передачі інформації чи її доступність також грають важливу роль, коли система повинна реагувати на зовнішній чи внутрішній збудник і формувати пакет даних для миттєвого відгуку. Особливо небезпечними для комп’ютерних мереж являються зловмисники, спеціалісти, професіонали в області обчислювальної техніки, які досконало володіють знаннями усіх переваг та слабких сторін обчислювальних мереж та систем і мають найсучасніші інструментальні та технологічні ресурси для аналізу та злому механізмів захисту корпоративних мереж. Дотримання правил захисту інформації не завжди допомагає в захищенні мережі. Корпоративні мережі висувають потребу в дослідженні нових методів захисту. Реалізації методів, алгоритмів, систем, які захищають важливі дані від стороннього несанкціонованого втручання легко знайдуть свого споживача. Кожна поважаюча себе та своїх споживачів компанія повинна мати в арсеналі своєї системи - СЗІ.

Тому метою даної дипломної роботи є створення системи захисту інформації в корпоративних мережах, яка б витримувала інтенсивні навантаження з боку різноманітних типів загроз інформації та захищала корпоративну мережу від неприпустимих збитків.

СЗІ — система захисту інформації;

КМ — корпоративна мережа;

НД — несанкціонований доступ;

XSS – Cross-site Scripting – міжсайтовий скриптинг;

SQL – Structured Query Language – структурована мова запитів;

Injection – ін’єкція;

RAID – Redundant Array of Inexpensive Disks or Drives – зайвий масив невикористаних дисків або приводів;

КС – комп’ютерна система;

НДІ – несанкціонований доступ до інформації;

Fishing – рибалка;

ЕОМ – електронно обчислювальна машина;

ЕЦП – електронно цифровий підпис;

МЕ – міжмережевий екран;

Firewall – міжмережевий екран, вогняна стіна, брандмауер;

Proxy – уповноважений;

ICF – internet connection firewall – міжмережевий екран інтернет з’єднання;

IP – internet protocol – протокол інтернету;

Stateful – наповнений станом (залежний від стану);

NGFW – next generation firewall – брандмауер наступного покоління;

DPI – deep package inspection – глибоке дослідження пакетів;

HTTP – hyper text transfer protocol – протокол передачі гіпертексту;

FTP – file transfer protocol – протокол передачі файлів;

NAT – network address translation – передачі мережевої адреси;

SMLI – stateful multilayer inspection – багатошарове залежне від стану дослідження;

CA – certificate authority – авторизація сертифікату;

SSL – secure sockets layer – рівень захищених сокетів;

Endpoint – кінцева точка;

URL – unified resource location – уніфіковане положення ресурсу;

НСД – найменший спільний дільник;

1 ПОСТАНОВКА ЗАДАЧІ

Під задачею для дипломної роботи розглядатиметься проектування та розробка системи захисту інформації корпоративної мережі.

Корпоративна мережа має бути відтворена з наступними властивостями:

- в мережі більше ніж декілька робочих станцій;
- мережа побудована за допомогою комутаторів та маршрутизаторів;
- має декілька сегментів;
- успішно функціонує без атак ззовні;
- містить захисний сегмент сконструйований за допомогою декількох мікросервісів.

Firewall, який захищатиме корпоративну мережу від атак має бути сконфігурованим на виконання наступних функцій та властивостей:

- захист мережі від XSS (Cross-Site Scripting);
- захист мережі від SQL Injection;
- виступати посередником між зовнішніми мережами та власне захищуваною корпоративною мережею;
- фільтрацію web-запитів, які не пройшли перевірку електронно цифрового підпису.

Мікросервіс перевірки електронно-цифрового ключа повинен виконувати наступні функції:

- перевірка електронно-цифрового підпису;
- генерація нових електронно-цифрових підписів.

Сегмент мережі, який буде виконувати роль атакуючої сторони, повинен

мати наступні властивості:

- генерує загрозу XSS (Cross-Site Scripting);
- генерує загрозу SQL Injection;
- не має безпосереднього доступу до корпоративної мережі.

Після проектування та розгортання системи, буде проведено стрес-тестування дослідження та аналіз результатів стрес тестування, дозволить зробити висновки про ефективність даної системи та можливість подальшої інтеграції в корпоративну мережу реального підприємства.

2 ОГЛЯД ПРЕДМЕТНОЇ ОБЛАСТІ ТА ІСНУЮЧИХ РІШЕНЬ

Проблема захисту інформації виникла в зв’язку зі створенням загального інформаційного простору та застосування комп’ютерів та комп’ютерних мереж у всіх сферах життя та життєдіяльності. Від обчислення суми на калькуляторі персонального комп’ютера до комплексних зборів даних з цілих комп’ютерних мереж і формування статистичних висновків.

Захистом інформації в комп’ютерних системах слід розуміти регулярне використання інструментів та методів, прийняття заходів з метою системного забезпечення надійності інформації, яка зберігається і оброблюється в комп’ютерних системах.

Під об’єктом захисту вважається інформація чи її носій або ж інформаційний процес по відношенню до якого потрібно встановити бажаний, виходячи з вирішуваної задачі, рівень безпеки.

Захист електронної інформації запобігає наступним видам інформаційних загроз:

- Відслідковування інформації;
- несанкціонований доступ неавторизованих користувачів;
- неправомірну використанню;
- пошкодження;
- знищення;
- спотворення;
- копіювання;
- Блокування.

Для того аби забезпечити відтворення захисту від перелічених вище загроз, комп’ютерна система повинна реалізовувати захист в:

- інформаційних носіях;
- технічних інструментах обробки;
- засобах передачі;

- методах обробки;
- базах даних.

Інформаційною безпекою називають захищеність інформації від незаконного ознайомлення, перетворення та знищення, а також захищеність ресурсів від впливу направленого на порушення їх роботоспроможності. Інформаційна безпека досягається шляхом забезпечення конфіденційності, цілісності, та достовірності оброблюваних даних, а також доступності і цілісності компонентів і ресурсів комп'ютерної системи.

Конфіденційність – приблизно еквівалентна приватності. Заходи, що вживаються для забезпечення конфіденційності, спрямовані на запобігання потраплянню конфіденційної інформації до тих людей, що знаходяться в неправильному стані, а також на те, щоб відповідні люди фактично отримали таку інформацію: Доступ повинен бути обмежений тим, хто має право переглядати дані дані. Загальновідомо також, щоб дані класифікувалися відповідно до кількості та типу збитків, які можна було б зробити, якщо вони потраплять у ненавмисні руки. Більш-менш жорсткі заходи можуть бути реалізовані відповідно до цих категорій.

Цілісність – передбачає підтримку послідовності, точності та достовірності даних протягом усього його життєвого циклу. Дані не повинні змінюватися під час транзиту, і необхідно вживати заходів для забезпечення того, щоб дані не могли бути змінені сторонніми особами (наприклад, у разі порушення конфіденційності). Ці заходи включають права доступу до файлів та засоби контролю доступу користувачів. Керування версіями може використовуватися для запобігання помилковим змінам або випадковому видаленню авторизованими користувачами. Крім того, мають бути використані деякі засоби для виявлення будь-яких змін у даних, які можуть виникнути внаслідок подій, не викликаних людиною, таких як електромагнітний імпульс (EMP) або аварія сервера. Деякі дані можуть включати контрольні суми, навіть криптографічні контрольні суми, для перевірки цілісності. Необхідно забезпечити резервні копії або надмірності для віднов-

лення відповідних даних у правильному стані.

Достовірність – це властивість інформації, яка виражається в суворій належності до суб’єкта, який є її джерелом, або тому суб’єкту, від якого ця інформація прийнята.

Найкраще забезпечити доступність можна завдяки ретельному обслуговуванню всіх апаратних засобів, негайному виконанню апаратного ремонту і підтримці правильно функціонуючого середовища операційної системи, вільного від конфліктів програмного забезпечення. Також важливо підтримувати всі необхідні оновлення системи. Не менш важливо забезпечити адекватну пропускну здатність зв'язку та запобігти виникненню вузьких місць. Надмірність, перехід на відмову, RAID-кластери навіть з високою доступністю можуть зменшити серйозні наслідки, коли виникають апаратні проблеми. Швидке та адаптивне відновлення після аварії є важливим для найгірших сценаріїв; ця здатність залежить від існування комплексного плану відновлення після аварії. Гарантії проти втрати даних або перебоїв у підключенні повинні включати непередбачувані події, такі як стихійні лиха та пожежа. Щоб запобігти втраті даних від таких випадків, резервну копію можна зберігати в географічно ізольованому місці, можливо, навіть у вогнезахисному, водонепроникному сейфі. Додаткове обладнання або програмне забезпечення безпеки, наприклад, брандмауери та проксі-сервери, можуть захищати від простоїв і недоступних даних через шкідливі дії, такі як атаки відмови в обслуговуванні та втручання мережі.

2.1 Загрози інформаційної безпеки

Щоб забезпечити ефективний захист інформації, необхідно в першу чергу розглянути та проаналізувати усі фактори, що можуть бути загрозою для інформаційної безпеки.

Загроза в контексті комп'ютерної безпеки стосується всього, що може завдати серйозної шкоди комп'ютерній системі. Загроза - це те, що може статися, а

може і не відбутися, але може призвести до серйозної шкоди. Загрози можуть призвести до атак на комп'ютерні системи, мережі та багато іншого. Загрози - це потенціали для того, щоб уразливості перетворилися на атаки на комп'ютерні системи, мережі та багато іншого. Вони можуть поставити під загрозу комп'ютерні системи та бізнес-комп'ютери окремих людей, тому уразливості повинні бути виправлені таким чином, щоб зловмисники не могли проникнути в систему та завдати шкоди.

Загрози можуть включати все, від вірусів, троянів, задніх дверей до прямих атак з боку хакерів. Часто термін "змішана загроза" є більш точним, оскільки більшість загроз пов'язано з численними подвигами. Наприклад, хакер може використовувати фішинг-атаку, щоб отримати інформацію про мережу та проникнути в мережу.

За природою виникнення розрізняють:

- природні загрози, викликані впливами на КС об'єктивних фізичних процесів або стихійних природних явищ;
- штучні загрози безпеки, викликані діяльністю людини.

Відповідно до положення джерела загроз. Джерело загроз може бути розташоване:

- поза контрольованої зони КС;
- в межах контрольованої зони КС;
- безпосередньо в КС.

За ступенем впливу на КС розрізняють:

- пасивні загрози, які при реалізації нічого не змінюють у структурі та змісті КС (загроза копіювання даних);
- активні загрози, які при впливі вносять зміни в структуру і зміст КС.

По етапах доступу користувачів або програм до ресурсів КС:

- загрози, які можуть проявлятися на етапі доступу до ресурсів КС;
- загрози, які проявляються після дозволу доступу (несанкціоноване використання ресурсів).

За поточним місцем розташування інформації в КС:

- загроза доступу до інформації на зовнішніх запам'ятовуючих пристроях, наприклад, копіювання даних з жорсткого диска;
- загроза доступу до інформації в оперативній пам'яті (несанкціоноване звернення до пам'яті);
- загроза доступу до інформації, що циркулює в лініях зв'язку (шляхом незаконного підключення).

За способом доступу до ресурсів КС:

- загрози, що використовують прямий стандартний шлях доступу до ресурсів за допомогою незаконно отриманих паролів або шляхом несанкціонованого використання терміналів законних користувачів;
- загрози, що використовують прихований нестандартний шлях доступу до ресурсів КС в обхід існуючих засобів захисту.

За ступенем залежності від активності КС розрізняють:

- загрози, які проявляються незалежно від активності КС (розкрадання носіїв інформації);
- загрози, які проявляються тільки в процесі обробки даних (поширення вірусів).

2.2 Види загроз

Всю множину потенційних загроз безпеки інформації в комп’ютерних системах можна розділити на 2 основних класи як зображено на рисунку 1.

Загрози, які не пов'язані з навмисними діями зловмисників і реалізуються у випадкові моменти часу, називають випадковими або ненавмисними. Механізм реалізації випадкових загроз в цілому досить добре вивчені, накопичений значний досвід протидії цим загрозам.

Стихійні лиха і аварії можуть призвести до найбільш руйнівних наслідків для КС, так як останні зазнають фізичного руйнування, інформація втрачається

або доступ до неї стає неможливий.

Збої і відмови складних систем неминучі. В результаті збоїв і відмов порушується працездатність технічних засобів, знищуються і спотворюються дані і програми, порушується алгоритм роботи пристроїв.

Помилки при розробці КС, алгоритмічні та програмні помилки приводять до наслідків, аналогічних наслідків збоїв і відмов технічних засобів. Крім того, такі помилки можуть бути використані зловмисниками для впливу на ресурси комп'ютерної системи.

Рисунок 1 - Загрози безпеки інформації в комп'ютерній системі. Клас 1 – випадкові, ненавмисні; Клас 2 – навмисні.

В результаті помилок користувачів і обслуговуючого персоналу порушення безпеки відбувається в 65% випадків. Некомпетентне, недбале або неуважне виконання функціональних обов'язків співробітниками приводить до знищення, порушення цілісності та конфіденційності інформації.

Навмисні загрози пов'язані з цілеспрямованими діями порушника. Даний клас загроз вивчений недостатньо, дуже динамічний і постійно поповнюється новими загрозами.

Методи і засоби шпигунства і диверсій найчастіше використовуються для отримання відомостей про систему захисту з метою проникнення в КС, а також для розкрадання і знищення інформаційних ресурсів. До таких методів відносять підслуховування, візуальне спостереження, розкрадання документів і машинних носіїв інформації, розкрадання програм і атрибутів системи захисту, збір і аналіз відходів машинних носіїв інформації, підпали.

Несанкціонований доступ – це коли хтось отримує доступ до веб-сайту, програми, сервера, служби або іншої системи, використовуючи чужий обліковий запис або інші методи. Наприклад, якщо хтось продовжував вгадувати пароль або ім'я користувача для облікового запису, який не був, доки не отримав доступ, він вважається несанкціонованим доступом. Несанкціонований доступ також може виникнути, якщо користувач намагається отримати доступ до зони системи, до якої вони не мають доступу. Під час спроби доступу до цієї області їм буде відмовлено у доступі та, можливо, побачить повідомлення про несанкціонований доступ.. Найбільш поширеними порушеннями є:

- перехоплення паролів - здійснюється спеціально розробленими програмами;
- «маскарад» - виконання будь-яких дій одним користувачем від імені іншого;
- незаконне використання привілеїв - захоплення привілеїв законних користувачів порушником.

Процес обробки і передачі інформації технічними засобами КС супроводжується електромагнітними випромінюваннями в навколишній простір і наведенням електричних сигналів в лініях зв'язку. Вони отримали назви побічних електромагнітних випромінювань і наведень. За допомогою спеціального обладнання сигнали приймаються, виділяються, посилюються і можуть або бути ви-

димим, або записуватися в пам'ятних пристроях. Електромагнітні випромінювання використовуються зловмисниками не тільки для отримання інформації, але і для її знищення.

Велику загрозу безпеці інформації в КС представляє несанкціонована модифікація алгоритмічної, програмної та технічної структур системи, яка отримала назву «закладка». Як правило, «закладки» впроваджуються в спеціалізовані системи і використовуються або для безпосереднього зловмисного впливу на КС, або для забезпечення неконтрольованого входу в систему.

Одним з основних джерел загроз безпеці є використання спеціальних програм, які отримали загальну назву «зловмисні програми». До таких програм відносяться:

- «комп'ютерні віруси» - подібні до вірусу грипу, призначений для розповсюдження від хоста до хоста і має можливість самостійно реплікації. Аналогічним чином, так само, як віруси грипу не можуть відтворюватися без стільникового вузла, комп'ютерні віруси не можуть розмножуватися та розповсюджуватися без програмування, наприклад, файлу або документа. Більш технічними термінами, комп'ютерний вірус - це тип шкідливого коду або програми, написаного для зміни способу роботи комп'ютера і призначеного для поширення з одного комп'ютера на інший. Вірус функціонує, вставляючи або прикріплюючи себе до законної програми або документа, який підтримує макроси, щоб виконати його код. У процесі роботи вірус може викликати непередбачувані або пошкоджуючі ефекти, такі як пошкодження системного програмного забезпечення шляхом пошкодження або знищення даних;
- «черв'яки» - це програми зловмисного програмного забезпечення, основна функція якої полягає в інфікуванні інших комп'ютерів, залишаючись активними на інфікованих системах. Комп'ютерний черв'як є самостійно копіюється шкідливим програмним забезпеченням, яке дублює себе для розповсюдження на неінфіковані комп'ютери. Черв'яки часто використовують частини операційної системи, які є автоматичними і невидимими для користувача. Для черв'яків

звичайно можна помітити лише тоді, коли їх неконтрольована реплікація споживає системні ресурси, уповільнює або зупиняє інші завдання;

- «троянські коні» в обчислювальній техніці - це програми, які здаються нешкідливими, але насправді шкідливі. Несподівані зміни в налаштуваннях комп'ютера та незвичайна активність, навіть якщо комп'ютер перебуває в режимі очікування, свідчать про те, що троянець перебуває на комп'ютері. Троянський кінь також може називатися вірусом троянського коня, але це технічно неправильно. На відміну від комп'ютерного вірусу, троянський кінь не може самостійно копіюватися, і не може розповсюджуватися без допомоги кінцевого користувача. Ось чому зловмисники повинні використовувати тактику соціальної інженерії, щоб змусити кінцевого користувача виконати троян. Як правило, програмне забезпечення шкідливого програмного забезпечення приховано в невинному вигляді в електронному вигляді або безкоштовно завантажується. Коли користувач натискає вкладення електронної пошти або завантажує безкоштовну програму, зловмисне програмне забезпечення, яке приховано всередині, передається на обчислювальний пристрій користувача. Потрапивши в систему, шкідливий код може виконати будь-яке завдання, яке зловмисник розробив для виконання.

Рисунок 2 – Статистика каналів витоку інформації за перший квартал 2008 року

Крім зазначених вище загроз безпеки на рисунку 2 [1], існує також загроза витоку інформації, яка з кожним роком стає все більш значущою проблемою безпеки. Щоб ефективно справлятися з витоками, необхідно знати яким чином вони відбуваються.

На чотири основні типи витоків доводиться переважна більшість (84%) інцидентів, причому половина цієї частки (40%) припадає на найпопулярнішу загрозу - крадіжку носіїв. 15% становить інсайд. До даної категорії відносяться інциденти, причиною яких стали дії співробітників, що мали легальний доступ до інформації. Наприклад, співробітник не мав права доступу до відомостей, але зумів обійти системи безпеки. Або інсайдер мав доступ до інформації і виніс її за межі організації. На хакерську атаку також припадає 15% загроз. У цю велику групу інцидентів потрапляють всі витоки, які сталися внаслідок зовнішнього вторгнення. Чи не занадто висока частка хакерських вторгнень пояснюється тим, що самі вторгнення стали менш помітними. 14% склала веб-витік. До цієї категорії потрапляють всі витоки, пов'язані з публікацією конфіденційних відомостей в загальнодоступних місцях, наприклад, в Глобальних мережах. 9% - це паперова витік.

Рисунок 3 – Статистика каналів витоку інформації за 2016 рік

Паперовим витоком є будь-який витік, який стався в результаті друку конфіденційних відомостей на паперових носіях. 7% складають інші. З графічним представленням даної статистики можна ознайомитися на рисунку 3 [2].

До цієї категорії потрапляють інциденти, точну причину яких встановити не вдалося, а також витоку, про які стало відомо постфактум, після використання персональних відомостей в незаконних цілях.

Крім того, в даний час активно розвивається фішинг – це тип атаки соціальної інженерії, яка часто використовується для крадіжки даних користувача, включаючи реєстраційні дані та номери кредитних карт. Це відбувається, коли зловмисник, маскується як довірена особа, обманює жертву у листі електронної пошти, миттєвого повідомлення або текстового повідомлення. Потім одержувач обманюється натисканням шкідливого посилання, яке може призвести до встановлення шкідливого програмного забезпечення, заморожування системи як частини атаки на вимогах або виявлення конфіденційної інформації. Атака може мати руйнівні результати. Для фізичних осіб це включає несанкціоновані покупки, викрадення коштів або ідентифікацію крадіжки. Крім того, фішинг часто ви-

користовується, щоб закріпитися в корпоративних або урядових мережах, як частина більшої атаки, наприклад, події, що розвиваються на постійній загрозі. У цьому останньому сценарії працівники компрометуються, щоб обійти периметри безпеки, поширити шкідливі програми в закритому середовищі або отримати привілейований доступ до захищених даних [3].

Не залежно від специфіки конкретних видів загроз, інформаційна безпека повинна зберігати цілісність, конфіденційність, доступність. Загрози порушення цілісності, конфіденційності та доступності є первинними. Порушення цілісності включає в себе будь-яка навмисна зміна інформації, що зберігається в КС або передається з однієї системи в іншу. Порушення конфіденційності може призвести до ситуації, коли інформація стає відомою тому, хто не має в своєму розпорядженні повноваження доступу до неї. Загроза недоступності інформації виникає щоразу, коли в результаті навмисних дій інших користувачів або зловмисників блокується доступ до деякого ресурсу КС.

Ще одним видом загроз інформаційної безпеці є загроза розкриття параметрів КС. В результаті її реалізації не заподіюється будь-яких збитків оброблюваної в КС інформації, але при цьому істотно посилюються можливості прояву первинних загроз [4].

2.3 Методи та засоби захисту інформації

2.3.1 Загальна характеристика засобів і методів захисту

Протидія численним загрозам інформаційної безпеки передбачає комплексне використання різних способів і заходів організаційного, правового, інженерно-технічного, програмно-апаратного, криптографічного характеру і т.п.

Організаційні заходи щодо захисту включають в себе сукупність дій по підбору і перевірки персоналу, який бере участь в підготовці і експлуатації програм та інформації, сувора регламентація процесу розробки і функціонування КС.

До правових заходів і засобів захисту відносяться діючі в країні закони, нормативні акти, які регламентують правила поводження з інформацією та відповідальність за їх порушення.

Інженерно-технічні засоби захисту досить різноманітні і включають в себе фізико-технічні, апаратні, технологічні, програмні, криптографічні та інші засоби. Дані засоби забезпечують наступні рубежі захисту: контрольована територія, будівля, приміщення, окремі пристрої разом з носіями інформації [5].

Програмно-апаратні засоби захисту безпосередньо застосовуються в комп'ютерах і комп'ютерних мережах, містять різні вбудовані в КС електронні, електромеханічні пристрої. Спеціальні пакети програм або окремі програми реалізують такі функції захисту, як розмежування і контроль доступу до ресурсів, реєстрація та аналіз процесів, що протікають, подій, користувачів, запобігання можливих руйнівних впливів на ресурси та інші. Суть криптографічного захисту полягає у приведенні (перетворення) інформації до неявного виду за допомогою спеціальних алгоритмів або апаратних засобів і відповідних кодових ключів.

2.3.2 Захист інформації від випадкових загроз

Для блокування (парирування) випадкових загроз безпеки в КС має бути вирішено комплекс завдань.

Дублювання інформації є одним з найбільш ефективних способів забезпечення цілісності інформації. Воно забезпечує захист інформації, як від випадкових загроз, так і від навмисних впливів. Для дублювання інформації можуть застосовуватися не тільки незнімні носії інформації або спеціально розроблені для цього пристрою, але і звичайні пристрої зі знімними машинними носіями. Поширеними методами дублювання даних в КС є використання виділених областей пам'яті на робочому диску і дзеркальних дисків (жорсткий диск з інформацією, ідентичною як на робочому диску) [6].

Рисунок 4 – Завдання для захисту інформації від випадкових загроз

Надійність є атрибутом будь-якого компонента, пов'язаного з комп'ютером (програмне забезпечення, або обладнання, або мережа, наприклад), що послідовно виконується відповідно до його специфікацій. Вже давно вважається одним з трьох пов'язаних атрибутів, які необхідно враховувати при оформленні, купівлі або використанні комп'ютерного продукту або компонента. Надійність, доступність і справність, для короткого - вважаються важливими аспектами для проектування в будь-яку систему. Теоретично надійний продукт абсолютно вільний від технічних помилок; однак на практиці постачальники часто виражають коефіцієнт надійності продукту у відсотках. Еволюційні продукти (ті, що розвивалися через численні версії протягом значного періоду часу) зазвичай вважаються все більш надійними, оскільки передбачається, що у попередніх випусках були усунені помилки. Наприклад, IBM z / OS (операційна система для їхніх серверів серії S / 390) має репутацію надійності, оскільки вона розвинулася з довгого ряду попередніх версій операційної системи MVS і OS / 390.Відмовостійкість - це властивість КС зберігати працездатність при відмовах окремих пристроїв, блоків, схем. Відомі три основні підходи до створення відмовостійких систем:

- просте резервування (використання пристроїв, блоків, вузлів, схем, тільки в якості резервних);
- завадостійке кодування інформації (робоча інформація доповнюється спеціальною контрольною інформацією-кодом, яка дозволяє визначати помилки і виправляти їх);
- створення адаптивних систем, які передбачають збереження працездатного стану КС при деякому зниженні ефективності функціонування в випадках відмов елементів.

Блокування помилкових операцій. Помилкові операції в роботі КС можуть бути викликані не тільки випадковими відмовами технічних і програмних засобів, але і помилками користувачів і обслуговуючого персоналу. Для блокування помилкових дій використовуються технічні та апаратно-програмні засоби, такі як блокувальні тумблери, запобіжники, засоби блокування записи на магнітні диски та інші [7].

Оптимізація. Одним з основних напрямків захисту інформації є скорочення числа помилок користувачів і персоналу, а також мінімізація наслідків цих помилок. Для досягнення цих цілей необхідні:

- наукова організація праці;
- виховання і навчання користувачів і персоналу;
- аналіз і вдосконалення процесів взаємодії людини і КС.

Мінімізація збитків. Запобігти стихійні лиха людина поки не в силах, але зменшити наслідки таких явищ у багатьох випадках вдається. Мінімізація наслідків аварій і стихійних лих для об'єктів КС може бути досягнута шляхом: правильного вибору місця розташування об'єкта (далеко від місць, де можливі стихійні лиха); обліку можливих аварій і стихійних лих при розробці та експлуатації КС; організації своєчасного оповіщення про можливі аварії; навчання персоналу боротьбі зі стихійними лихами і аваріями, методам ліквідації їх наслідків.

2.3.3 Захист КС від несанкціонованого втручання

Основним способом захисту від зловмисників вважається впровадження так званих засобів ААА, або 3А (аутентифікація, авторизація, адміністрування).

Авторизація (санкціонування, дозвіл) - процедура, за якою користувач при вході в систему розпізнається і отримує права доступу, дозволені системним адміністратором, до обчислювальних ресурсів (комп'ютерів, дисків, папок, периферійних пристроїв).

Авторизація виконується програмою і включає в себе ідентифікацію та аутентифікацію.

Ідентифікація – це логічна сутність, яка використовується для ідентифікації користувача на програмному забезпеченні, системі, веб-сайті або в будь-якому загальному IT-середовищі. Він використовується в будь-якій системі, що підтримує IT, для виявлення та розрізнення користувачів, які мають доступ або використовують його. Ідентифікатор користувача також може називатися ім'ям користувача або ідентифікатором користувача.

Аутентифікація – це процес визначення того, хто чи щось є, насправді, хто або що він декларує себе. Технологія перевірки автентичності забезпечує контроль доступу для систем, перевіряючи, чи облікові дані користувача збігаються з обліковими даними в базі даних авторизованих користувачів або на сервері автентифікації даних. Користувачі, як правило, ідентифікуються з ідентифікатором користувача, а аутентифікація виконується, коли користувач надає облікові дані, наприклад пароль, який відповідає цьому ідентифікатору користувача. Більшість користувачів найбільш знайомі з використанням пароля, який, як частина інформації, яка повинна бути відома тільки користувачеві, називається фактором аутентифікації знань. Найбільш часто вживаними методами авторизації є методи, засновані на використанні паролів (секретних послідовностей символів). Пароль можна встановити на запуск програми, окремі дії на комп'ютері або в мережі. Крім паролів для підтвердження автентичності можуть використовуватися плас-

тикові картки та смарт-карти.

Адміністрування - це реєстрація дій користувача в мережі, включаючи його спроби доступу до ресурсів. Для своєчасного припинення несанкціонованих дій, для контролю за дотриманням встановлених правил доступу необхідно забезпечити регулярний збір, фіксацію і видачу за запитами відомостей про всі звернення до захищених комп'ютерних ресурсів. Основною формою реєстрації є програмне ведення спеціальних реєстраційних журналів, що представляють собою файли на зовнішніх носіях інформації.

Найчастіше витік інформації відбувається шляхом несанкціонованого копіювання інформації. Ця загроза блокується:

- методами, що ускладнюють зчитування скопійованої інформації. Засновані на створенні в процесі запису інформації на відповідні накопичувачі таких особливостей (нестандартна розмітка, форматування, носія інформації, установка електронного ключа), які не дозволяють зчитувати отриману копію на інших накопичувачах, що не входять до складу захищеної КС. Іншими словами, ці методи спрямовані на забезпечення сумісності накопичувачів тільки всередині даної КС;
- методами, що перешкоджають використанню інформації. Ускладнюють використання отриманих копіюванням програм і даних. Найбільш ефективним в цьому відношенні засобом захисту є зберігання інформації в перетвореному криптографічними методами вигляді. Іншим методом протидії несанкціонованому виконання скопійованих програм є використання блоку контролю середовища розміщення програми. Він створюється при інсталяції програми і включає характеристики середовища, в якому розміщується програма, а також засоби порівняння цих характеристик. В якості характеристик використовуються характеристики ЕОМ або носія інформації.

Для захисту КС від різноманітних зловмисних програм (вірусів) розробляються спеціальні антивірусні засоби.

Антивірусна програма – це клас програм, призначений для запобігання,

виявлення та видалення шкідливих інфекцій на окремих обчислювальних пристроях, мережах та IT-системах. Антивірусне програмне забезпечення, спочатку розроблене для виявлення та видалення вірусів з комп'ютерів, також може захищати від різноманітних загроз, включаючи інші типи шкідливого програмного забезпечення, такі як клавіатурні шпигуни, викрадачі браузерів, троянські коні, черв'яки, руткіти, шпигунські програми, рекламні програми, бот-мережі та вимогам.. Існує кілька різновидів антивірусних програм:

- сканери або програми-фаги - це програми пошуку в файлах, пам'яті, завантажувальних секторах дисків сигнатур вірусів (унікального програмного коду саме цього вірусу), перевіряють і лікують файли;
- монітори (різновид сканерів) - перевіряють оперативну пам'ять при завантаженні операційної системи, автоматично перевіряють всі файли в момент їх відкриття і закриття, щоб не допустити відкриття і запис файлу, зараженого вірусом; блокує віруси;
- іммунізатори - запобігають зараженню файлів, виявляють підозрілі дії при роботі комп'ютера, характерні для вірусу на ранній стадії (до розмноження) і посилають користувачеві відповідне повідомлення;
- ревізори - запам'ятовують початковий стан програм, каталогів до зараження і періодично (або за бажанням користувача) порівнюють поточний стан з вихідним;
- лікарі - не тільки знаходять заражені вірусами файли, але і «лікують» їх, тобто видаляють з файлу тіло програми-вірусу, повертаючи файли в початковий стан;
- блокувальники - відстежують події і перехоплюють підозрілі дії (вироблені шкідливою програмою), забороняють дію або запитують дозвіл користувача.

2.4 Криптографічні методи захисту інформації та міжмережеві екрани

Ефективним засобом протидії різним загрозам інформаційної безпеки є закриття інформації методами криптографічного (від грец. Kryptos - таємний) перетворення. У результаті такого перетворення захищувана інформація стає недоступною для ознайомлення і безпосереднього використання особами, які не мають на це повноважень. По виду впливу на вихідну інформацію криптографічні методи розділені на наступні види.

Шифрування – це метод, за допомогою якого відкритий текст або будь-який інший тип даних перетворюється з читаної форми в закодовану версію, яку можна декодувати тільки іншим об'єктом, якщо вони мають доступ до ключа дешифрування. Шифрування є одним з найважливіших методів забезпечення безпеки даних, особливо для захисту даних, що передаються через мережі. Шифрування широко використовується в Інтернеті для захисту інформації користувача, що передається між браузером і сервером, включаючи паролі, платіжну інформацію та іншу особисту інформацію, яку слід вважати приватною. Організації та окремі особи також зазвичай використовують шифрування для захисту конфіденційних даних, що зберігаються на комп'ютерах, серверах і мобільних пристроях, таких як телефони або планшети.

Стеганографія - метод захисту комп'ютерних даних, переданих по каналах телекомунікацій, шляхом приховування повідомлення серед відкритого тексту, зображення або звуку в файлі-контейнері. Дозволяє приховати не тільки зміст зберігається або передається, але і сам факт зберігання або передачі закритої інформації. Прихований файл може бути зашифрований. Якщо хтось випадково виявить прихований файл, то зашифрована інформація буде сприйнята як збій в роботі системи.

Кодування - заміна смислових конструкцій вихідної інформації (слів, пропозицій) кодами. Коди можуть бути використані як сполучення букв, цифр. При кодуванні і зворотному перетворенні використовуються спеціальні таблиці або словники, що зберігаються в секреті. Кодування широко використовується для захисту інформації від спотворень в каналах зв'язку.

Метою стиснення інформації є скорочення обсягів інформації. У той же час стисла інформація не може бути прочитана або використана без зворотного перетворення. З огляду на доступність засобів стиснення і зворотного перетворення, ці методи не можна розглядати як надійні засоби криптографічного перетворення інформації. Тому стислі файли піддаються подальшого шифрування.

Розсічення-рознесення полягає в тому, що масив даних, що захищаються ділиться (розтинають) на такі елементи, кожен з яких окремо не дозволяє розкрити зміст інформації, що захищається. Виділені таким чином елементи даних розносяться по різних зонах ЗП або розташовуються на різних носіях.

Електронний цифровий підпис (ЕЦП) – це математичний метод, який використовується для перевірки достовірності та цілісності повідомлення, програмного забезпечення або цифрового документа. Цифровий еквівалент рукописного підпису або штампованої печатки, цифрового підпису дає набагато більш притаманну безпеку, і він призначений для вирішення проблеми фальсифікації та уособлення в цифрових комунікаціях. Цифрові підписи можуть надавати додаткові гарантії щодо підтвердження походження, ідентичності та статусу електронного документа, транзакції або повідомлення і можуть підтвердити інформовану згоду підписувача. У багатьох країнах, включаючи Сполучені Штати, цифрові підписи вважаються юридично обов'язковими так само, як і традиційні підписи документів. Видавництво Уряду Сполучених Штатів публікує електронні версії бюджету, державних і приватних законів, а також конгресові законопроекти з цифровими підписами.

Для блокування загроз, що виходять із загальнодоступної системи, використовується спеціальне програмне або апаратно-програмний засіб, яке отримало назву міжмережевий екран (МЕ) або firewall. МЕ дозволяє розділити загальну мережу на дві частини або реалізувати набір правил, що визначають умови проходження пакетів з даними через кордон з однієї частини загальної мережі в іншу. Іноді мережевий захист повністю блокує трафік зовні всередину, але дозволяє внутрішнім користувачам вільно зв'язуватися із зовнішнім світом. Зазвичай

МЕ захищають внутрішню мережу підприємства від вторгнень з глобальної мережі Інтернет. Брандмауер виконує чотири основні функції:

- фільтрація даних на різних рівнях;
- використання екрануючих агентів (proxy-сервери), які є програмами-посередниками і забезпечують з'єднання між суб'єктом і об'єктом доступу, а потім пересилають інформацію, здійснюючи контроль і реєстрацію;
- трансляція адрес - призначена для приховування від зовнішніх абонентів справжніх внутрішніх адрес;
- реєстрація подій в спеціальних журналах. Аналіз записів дозволяє зафіксувати спроби порушення встановлених правил обміну інформацією в мережі і виявити зловмисника.

2.5 Firewall (Брандмауер)

Загалом, комп'ютерний брандмауер - це програма, яка запобігає несанкціонованому доступу до приватної мережі або з неї. Брандмауери - це інструменти, які можна використовувати для підвищення безпеки комп'ютерів, підключених до мережі, наприклад, локальної мережі або Інтернету. Вони є невід'ємною частиною комплексної системи безпеки для вашої мережі.

Брандмауер повністю ізолює комп'ютер від Інтернету, використовуючи «стіну коду», яка перевіряє кожен окремий «пакет» даних, коли він надходить з будь-якої сторони брандмауера - вхідний або вихідний з комп'ютера - щоб визначити, чи потрібно пропустити або заблокувати пакети.

Брандмауери мають можливість додатково підвищувати безпеку, надаючи можливість гранульованого контролю за типом системних функцій і процесів, які мають доступ до мережевих ресурсів. Ці брандмауери можуть використовувати різні типи підписів і умови хоста, щоб дозволити або заборонити трафік. Хоча вони звучать складно, брандмауери відносно легко встановлюються, налаштовуються і працюють.

Більшість людей вважає, що брандмауер є пристроєм, встановленим у мережі, і він контролює трафік, який проходить через сегмент мережі.

Тим не менш, ви можете мати хост на основі брандмауерів. Це може бути виконано на самих системах, таких як ICF (Internet Connection Firewall). В основному, робота обох брандмауерів однакова: зупинити вторгнення і забезпечити надійний метод політики контролю доступу. У простому визначенні брандмауери - це не що інше, як система, яка захищає ваш комп'ютер.

2.5.1 Як працює брандмауер?

Брандмауери ретельно аналізують вхідний трафік на основі заздалегідь встановлених правил і фільтрують трафік, що надходить із незабезпечених або підозрілих джерел, щоб запобігти атакам. Брандмауери охороняють трафік у точці входу комп'ютера, яка називається портами, де відбувається обмін інформацією з зовнішніми пристроями. Наприклад, «адресі джерела 172.18.1.1 дозволено дістатися до пункту 172.18.2.1 через порт 22.»

Подумайте про IP-адреси як про будинки, а номери портів - як про кімнати в будинку. Лише довіреним особам (вихідним адресам) дозволяється взагалі вводити будинок (адреса призначення), а потім додатково фільтруватись, щоб люди в будинку мали доступ лише до певних номерів (портів призначення), залежно від того, чи є вони власником , дитини або гостя. Власник дозволений в будь-який номер (будь-який порт), а діти і гості допускаються до певного набору номерів (конкретні порти).

2.6 Типи брандмауерів

Брандмауери можуть бути як програмними, так і апаратними, хоча найкраще мати обидва. Програмний брандмауер - це програма, встановлена на кожному комп'ютері і регулює трафік через номери портів і програми, а фізичний

брандмауер - це частина обладнання, встановленого між вашою мережею і шлюзом.

Брандмауери з фільтрацією пакетів, найпоширеніший тип брандмауера, досліджують пакети та забороняють їм проходити, якщо вони не відповідають встановленому набору правил безпеки. Цей тип брандмауера перевіряє вихідні та цільові IP-адреси пакета. Якщо пакети збігаються з правилами «дозволеного» правила на брандмауері, то довірятимуть входу в мережу.

Брандмауери фільтрації пакетів поділяються на дві категорії: державні та безгромадські. Брандмауери без паспортизації досліджують пакети незалежно один від одного і не мають контексту, що робить їх легкими об'єктами для хакерів. На відміну від цього, брандмауери типу stateful запам'ятовують інформацію про раніше передані пакети і вважаються набагато більш безпечними.

Хоча брандмауери з фільтрацією пакетів можуть бути ефективними, вони в кінцевому підсумку забезпечують дуже простий захист і можуть бути дуже обмеженими - наприклад, вони не можуть визначити, чи зміст надісланого запиту негативно вплине на програму. Якщо зловмисний запит, дозволений з адреси надійного джерела, призведе до видалення бази даних, брандмауер не матиме можливості дізнатися про це. Брандмауери наступного покоління та брандмауери-проксі-пристрої більш оснащені для виявлення таких загроз.

Брандмауери наступного покоління (NGFW) поєднують традиційну технологію брандмауера з додатковими функціональними можливостями, такими як зашифрована перевірка трафіку, системи запобігання вторгнення, антивірус та багато іншого. Зокрема, вона включає глибоку перевірку пакетів (DPI). Хоча базові брандмауери розглядають лише заголовки пакетів, глибока перевірка пакетів перевіряє дані в самому пакеті, дозволяючи користувачам більш ефективно ідентифікувати, класифікувати або зупиняти пакети з шкідливими даними.

Проксі-брандмауери фільтрують мережевий трафік на рівні програми. На відміну від основних брандмауерів, проксі виступає посередником між двома кінцевими системами. Клієнт повинен надіслати запит до брандмауера, де він

потім оцінюється з урахуванням набору правил безпеки, а потім дозволено або заблоковано. Зокрема, проксі-брандмауери відстежують трафік для протоколів шару 7, таких як HTTP і FTP, і використовують як перевірку статусу, так і глибокий пакет для виявлення шкідливого трафіку.

Мережеві брандмауери мережевих адрес дозволяють декільком пристроям з незалежними мережевими адресами підключатися до Інтернету, використовуючи одну IP-адресу, зберігаючи приховані окремі IP-адреси. Як наслідок, зловмисники, які сканують мережу для IP-адрес, не можуть зафіксувати конкретні деталі, забезпечуючи більшу безпеку від атак. Брандмауери NAT подібні до брандмауерів-проксі, оскільки вони виступають посередником між групою комп'ютерів і зовнішнім трафіком.

Блоки міжмережевих брандмауерів з багатошаровою перевіркою (SMLI) фільтрують пакети в мережевих, транспортних і прикладних шарах, порівнюючи їх з відомими надійними пакетами. Як і брандмауери NGFW, SMLI також перевіряє весь пакет і тільки дозволяє їм пройти, якщо вони передають кожен шар окремо. Ці брандмауери досліджують пакети, щоб визначити стан зв'язку (таким чином, ім'я), щоб переконатися, що всі ініційовані комунікації відбуваються тільки з надійними джерелами.

2.7 Електронно-цифровий підпис

Цифровий підпис - це процес, який гарантує, що зміст повідомлення не було змінено під час транспортування.

Коли сервер, цифрово підписуєте документ, додається односторонній хеш (шифрування) вмісту повідомлення за допомогою пари публічних і приватних ключів.

Отримувач все ще може прочитати його, але процес створює «підпис», який може розшифрувати лише відкритий ключ сервера. Отримувач, використовуючи відкритий ключ сервера, може потім перевірити відправника, а також ці-

лісність вмісту повідомлення.

Незалежно від того, чи є це електронна пошта, онлайн-замовлення або фотографія на водяних знаках на eBay, якщо передача надходить, але цифровий підпис не відповідає відкритому ключу цифрового сертифіката, то отримувач знає, що повідомлення було змінено.

2.7.1 Як працює електронно-цифровий підпис?

Цифровий підпис можна розглядати як числове значення, яке представлено у вигляді послідовності символів. Створення цифрового підпису є складним математичним процесом, який може бути створений тільки комп'ютером.

Розглянемо сценарій, коли Аліса повинна підписати файл або електронну пошту в електронному вигляді та надіслати його Бобу.

1. Аліса вибирає файл для цифрового підпису.
2. Хеш-значення вмісту файлу або повідомлення обчислюється комп'ютером Аліси.
3. Це значення хешу зашифровано за допомогою ключа підпису Аліси (який є приватним ключем) для створення цифрового підпису.
4. Тепер оригінальний файл або повідомлення електронної пошти разом з цифровим підписом надсилаються Бобу.
5. Після того, як Боб отримає підписане повідомлення, відповідна програма (наприклад, програма електронної пошти) визначає, що повідомлення було підписано. Комп'ютер Боба переходить до:
    1) Розшифруйте цифровий підпис за допомогою відкритого ключа Аліси.
    2) Розрахуйте хеш вихідного повідомлення.
    3) Порівняйте (a) хеш, який він обчислив з отриманого повідомлення з розшифрованим хешем (b), отриманим з повідомленням Аліси.

6. Будь-яка різниця у значеннях хеша виявить підроблення повідомлення.

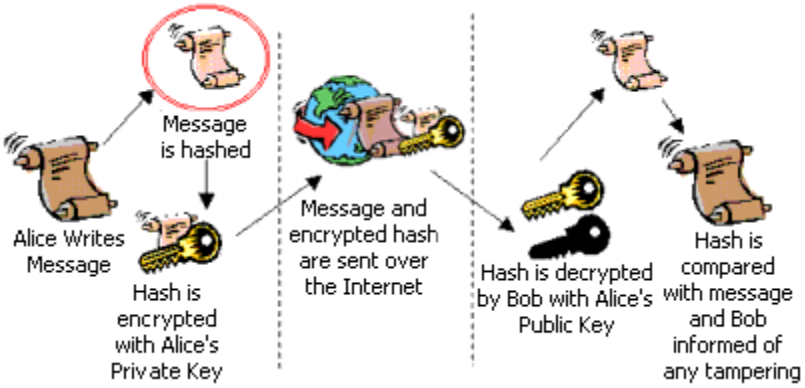

Рисунок 5 – Алгоритм роботи електронно-цифрового підпису проілюстрований в абстрактній формі

2.7.2 Як створити цифровий підпис?

Отримати цифровий підпис можна з авторитетного органу сертифікації, такого як Sectigo, або створити його самостійно. Для цифрового підписання документа потрібен цифровий сертифікат. Однак, якщо створити та використовувати самостійно підписаний сертифікат, одержувачі ваших документів не зможуть перевірити автентичність цифрового підпису. Отримувачам доведеться вручну довіряти самостійно підписаному сертифікату.

Якщо є потреба в тому, щоб одержувачі документів могли перевірити автентичність цифрового підпису, потрібно отримати цифровий сертифікат від авторитетного CA. Після завантаження та встановлення сертифіката - потрібно використовувати кнопки «Знак» і «Шифрувати» на поштовому клієнті для шифрування та цифрового підпису електронних листів. Це має більше сенсу в бізнес-сценарії, оскільки він запевняє одержувача, що він справді надісланий вами, а не певним самозванцем.

2.7.3 Інші використання цифрового підпису

Іноді потрібні докази того, що документ прийшов від вас, і ніхто не приручив його, оскільки ви його надіслали. Цифровий підпис з вашим сертифікатом SSL заповнює рахунок.

З іншого боку, іноді потрібно довести, що документ прийшов від когось іншого і не був змінений на цьому шляху. Наприклад, у юридичних питаннях, можливо, доведеться довести, що контракт не був змінений, оскільки хтось надіслав його як електронний лист.

Оскільки комп'ютер постійно з'єднує цифровий підпис з однією збереженою версією документа, майже неможливо відмовитися від цифрового підпису.

Або, якщо ви розробник, який розповсюджує програмне забезпечення в Інтернеті, вам може знадобитися запевнити своїх клієнтів, що ваші виконувані файли дійсно від вас. Помістіть сертифікат підпису коду у свій інструментарій.

2.7.4 Типи цифрових підписів

Різні платформи обробки документів підтримують і дозволяють створювати різні типи цифрових підписів.

- Adobe підтримує - сертифіковані та затверджені цифрові підписи;
- Microsoft Word підтримує - видимі та невидимі цифрові підписи.

2.7.4.1 Сертифіковані підписи

Додавання підтверджуючого підпису до PDF-документа вказує, що ви є автором документа і хочете захистити документ від підробки.

Сертифіковані документи PDF відображають унікальну блакитну стрічку у верхній частині документа. Він містить ім'я підписувача документа і видавця

сертифіката для вказівки авторства та автентичності документа.

2.7.4.2 Підписи схвалення

Підписи схвалення на документі можна використовувати в робочому процесі вашої організації. Вони допомагають оптимізувати процедуру затвердження вашої організації. Процес передбачає збір схвалень, зроблених вами та іншими особами, і вбудовування їх у документ PDF.

Adobe дозволяє підписи включати такі деталі, як зображення вашого фізичного підпису, дату, місцезнаходження та офіційну печатку.

2.7.4.3 Видимі цифрові підписи

Видимі цифрові підписи дозволяють одному або декільком користувачам цифрово підписати один документ. Підписи будуть відображатися в документі так само, як підписи застосовуються до фізичного документа.

2.7.4.4 Невидимі цифрові підписи

Документи з невидимими цифровими підписами несуть візуальну індикацію блакитної стрічки на панелі завдань. Ви можете використовувати невидимі цифрові підписи, коли вам не потрібно або не бажаєте відображати свій підпис, але ви повинні надати вказівки на автентичність документа, його цілісність і його походження.

2.8 Огляд існуючих рішень

Перед початком планування та розробки власної реалізації, розглянемо декілька варіантів існуючих рішень в галузі захисту інформації корпоративних ме-

реж. Зокрема, додатки для аналізу вразливостей, додатки для убезпечення мереж.

2.8.1 Веб сервіс Webroot SecureAnywhere Endpoint Protection

Webroot SecureAnywhere Endpoint Protection забезпечує багатовекторний захист від вірусів і шкідливих програм, що надають повний захист від усіх сучасних шкідливих загроз, включаючи трояни, клавіатурні шпигуни, фішинг, шпигунські програми, зворотні двері, руткіти, нульові та постійні загрози. Вбудований ідентифікаційний і конфіденційний щит припиняє крадіжку або захоплення даних при використанні Інтернету, а вихідний брандмауер також зупиняє злодійські дані. Немає необхідності турбуватися або запускати оновлення засоби безпеки, керовані хмарою, кінцеві точки завжди актуальні.

Для того, щоб скористатися можливостями даного захисного додатку з початку потрібно пройти реєстрацію на офіційному сайті додатку. Після створення облікового запису, під час першого входу в консоль, потрібно вибрати відповідну конфігурацію сайту. Потрібно лише вибрати консоль під час першого входу в систему після створення облікового запису. Щоб вибрати консоль:

1. Потрібно увійти до консолі керування (Відобразиться вікно вибору консолі) як на рисунку 6 [8].
2. Якщо потрібне керування пристроями для своєї компанії та використання єдиного коду для всіх пристроїв, можна вибрати Бізнес консоль.

Рисунок 6 – Вікно вибору консолі

2.8.2 Налаштування бізнес консолі

Після створення облікового запису та вибору консолі керування бізнесом потрібно ввести інформацію про компанію. Щоб налаштувати бізнес-консоль:

1. Після вибору консолі керування бізнесом відобразиться сторінка бізнес-інформації.

Рисунок 7 – Сторінка бізнес-інформації

2. У полі Назва сайту / компанії потрібно ввести назву сайту чи компанії.

3. У полі Кількість пристроїв ввести кількість пристроїв, якими потрібно буде керувати.

4. У спадному меню «Промисловість компанії» виберіть тип галузі, яка найкраще відображає вашу компанії.

5. У спадному меню Розмір компанії виберіть діапазон, який найкраще відображає кількість співробітників у вашій компанії.

6. Після цього натиснути кнопку Вибрати.

7. Відображається панель інструментів для компанії. Тут можна виконати такі дії:

- переглянути бізнес-прожектор, який завжди доступний у спадному меню Довідка (?);
- перейти до захисту кінцевої точки;
- керівництво з адміністрування захисту.

8. За необхідності ви можете редагувати інформацію своєї компанії. Додаткову інформацію див. У розділі Перегляд та редагування.

Рисунок 8 – Вигляд справно працюючого, сконфігурованого додатку

Виходячи з представленого функціоналу можна зробити висновки, що даний додаток не має універсальності і великої швидкості вбудування в систему, має захист від загроз такого ж типу як і досліджується в даній дипломній роботі, але відкритих кодів реалізації для цього додатку знайти не вийшло, тому і проаналізувати, наскільки однаково чи по різному працює СЗІ даної дипломної роботи з існуючою СЗІ також не вийде.

2.8.3 ManageEngine Firewall Analyzer

Firewall Analyzer є агентом меншої лог-аналітики і управління конфігурацією програмного забезпечення, яке аналізує логи з брандмауерів і генерує спо-

віщення в режимі реального часу оповіщення, безпеки і пропускної здатності звітів. Рішення - це програмне забезпечення постачальника-агностика і підтримує більше 50 постачальників брандмауера. Вона також надає можливість адміністраторам надавати вичерпні звіти про події безпеки і, в свою чергу, вони можуть вживати заходів для пом'якшення безпеки.

Можливості мережевої безпеки:

- переглянути повний список програмного забезпечення мережевої безпеки;
- антиспам;
- антивірус;
- захист електронної пошти;
- відстеження подій;
- система виявлення вторгнень;
- IP захист;
- відповідь на загрозу;
- сканування вразливості;
- управління веб-загрозами;
- звітність про веб-трафік.

Окрім завантаження, встановлення та вибору бажаної підтримуваної бази даних, даний додаток не потребує додаткових конфігурацій, що є надзвичайним плюсом. Ознайомитися з вікном входу в додаток можна на рисунку 9 [9].

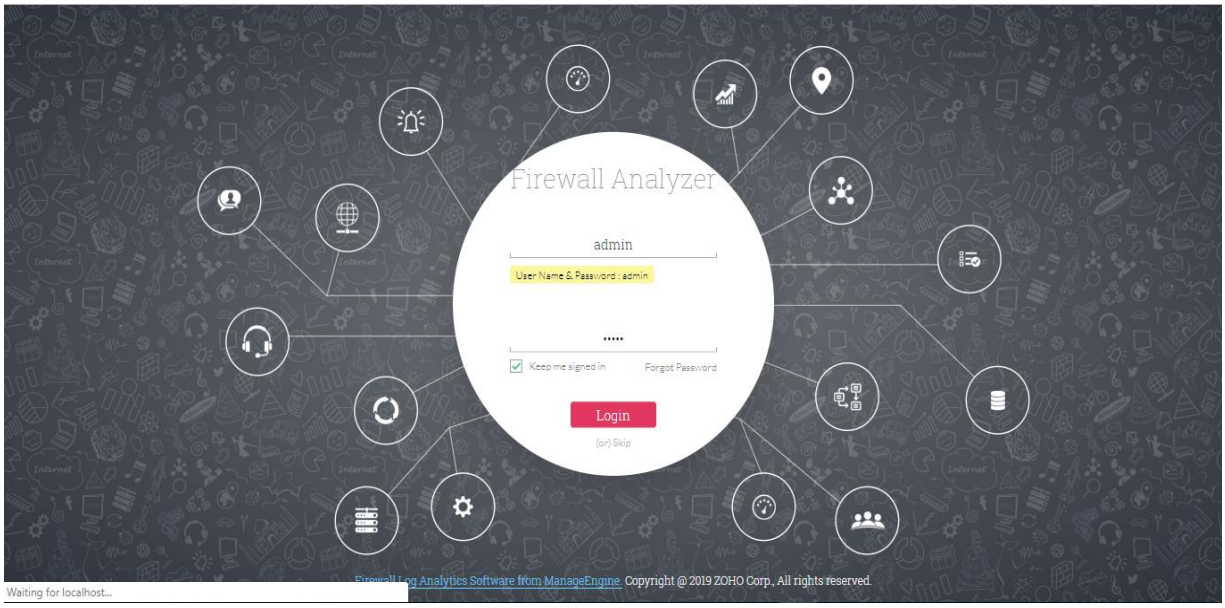

Рисунок 9 – Вікно входу в додаток

На вікні вибору конфігурацій для досліджуваної галузі можна провести конфігурацію:

1. Add Device (Додавання приладу) – додавання приладу тестування на загрози;
2. Prerequisite (передумови) – можливість додавання версії девайсів, використовуваних баз даних і т. д;
3. Real Time Alerts (Сповіщення в реальному часі) – вибір в якому форматі, в який додаток і як буде проводиться сповіщення порушення безпеки;
4. Custom Reports (Користувацькі звіти) – Можливість вказання власного формату звітів;
5. Rule/Policy Management (Управління Правилами/Політиками).

Дані конфігурації допомагають поліпшити користувацький досвід з вебсервісом. Можливість користувацького налаштування через UI (User Interface – користувацький інтерфейс) є великим плюсом, адже у більшості додатків чи плагінів для захисту мереж або додатків мереж конфігурація захисних механізмів та екранів, виводу логування та інших налаштування виконується або під час завантаження або через консольні додатки за допомогою консольних команд. В ManageEngine також доступна можливість зміни конфігурацій, після їх виходу з ра-

мок вимог до захисту, також через UI.

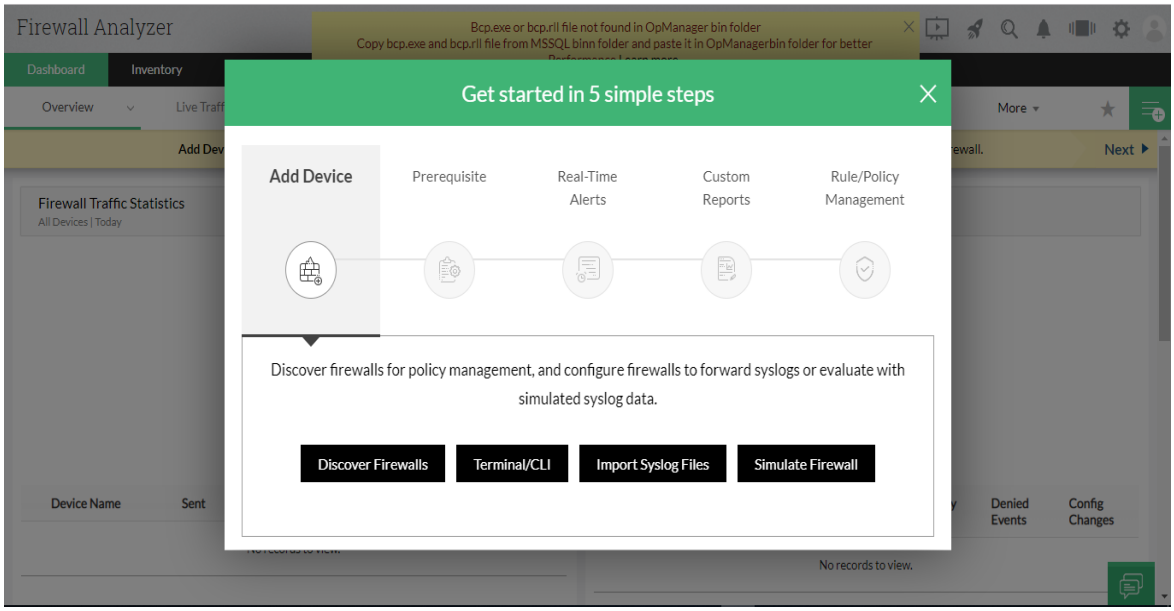

Рисунок 10 – Вікно користувацького налаштування додатку захисту

Спробуємо просимулювати захисний процес за допомогою відповідного пункту меню. Відкривши вікно конфігурації Firewall-а (дивитися рисунок 11) можемо виконати різноманітні налаштування починаючи від імені постачальника (Vendor Name) до протоколу взаємодії.

Переглянути вже налаштовані Firewall-и можна у вікні Inventory (дивитися рисунок 12) (Інвентар).

Просимулювавши захисний процес в ManageEngine можна ознайомитися зі звітом на рисунок 13, в якому буде вказана інформація про країну з якої надійшов запит, кількість байтів переданої та відправленої інформації та статистичну діаграму цих показників.

Отже підводячи підсумки, MangeEngine дуже гнучкий додаток, з різноманітними можливостями налаштування (рисунок 11 [2]) основною задачею якого є вбудування Firewall-ів в існуючі системи і аналіз трафіку.

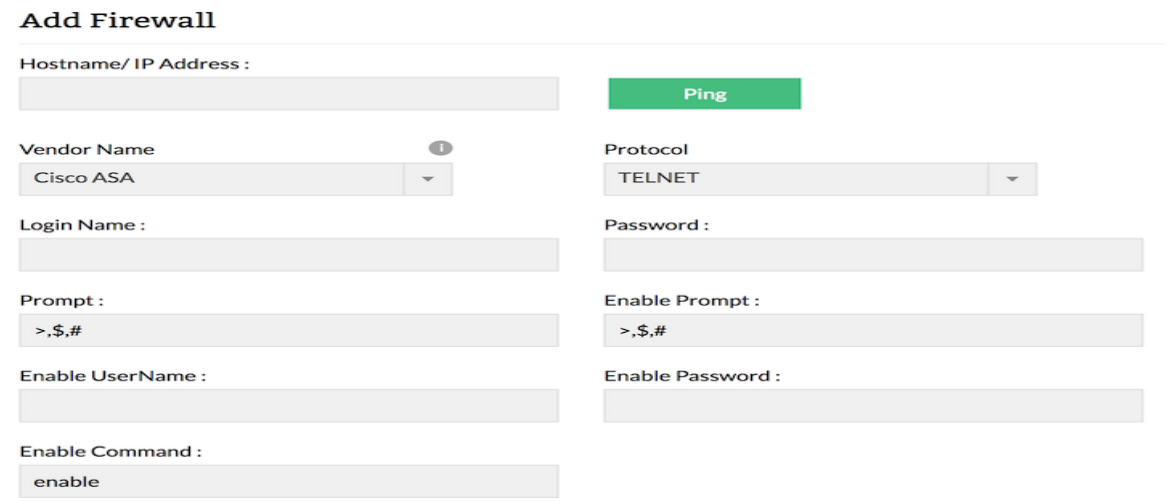

Рисунок 11 – Вікно налаштування Firewall-у

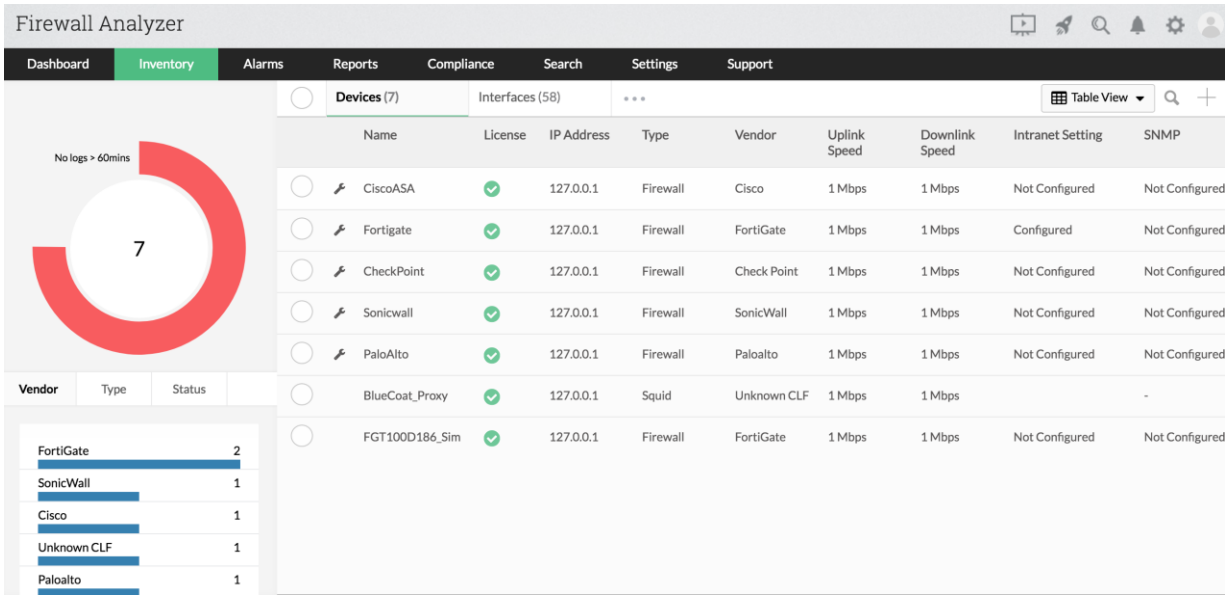

Рисунок 12 – Вікно інвентаря Firewall-ів

Дані задачі, які виконує додаток підходять до мети даної дипломної роботи частково, тільки можливістю налаштування гарно представлених звітів. Тому виконання даного дипломного проекту є актуальним.

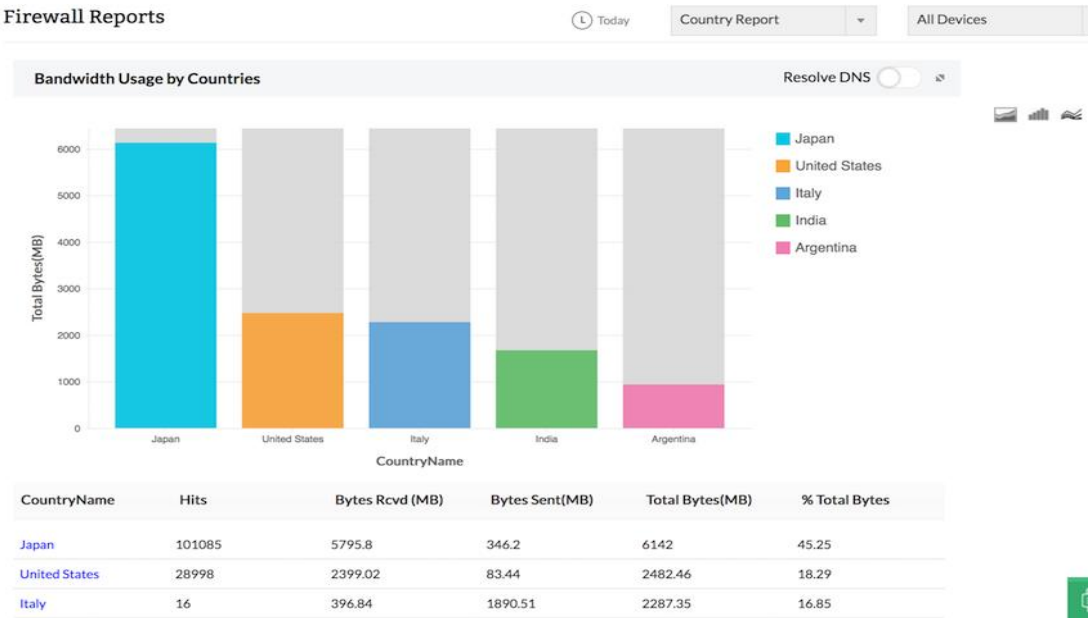

Рисунок 13 – Вікно звіту про пройдену крізь Firewall інформацію

3 ОБГРУНТУВАННЯ ВИБОРУ ТА РЕАЛІЗАЦІЯ

3.1 Обґрунтування вибору

Підсумовуючи вимоги та мету даної дипломної роботи виведемо основні положення та характеристики розроблюваної системи захисту. Система повинна легко вбудовуватися в існуючі мережі. Швидко розгортуваною. Забезпечувати захист від загроз типу XSS та SQL Injection. Надавати коротку змістовну інформацію про дії виконані для придушення загрозливого запиту або проходження звичайного запиту в мережу.

Для виконання вимоги легкого вбудування була обрана технологія ASP.NET Core, яка дозволить розгорнути розроблену систему на робочих станціях чи серверах з операційними системами (Windows, Linux, macOS) або в Docker.

Для виконання вимоги забезпечення захисту від XSS та SQL Injection були розроблені механізми захисту в середини мікросервісу Firewall, як були виконані за допомогою тієї ж технології ASP.NET Core фреймворку. Деякі елементи захисту реалізовані також реалізовані в середині мікросервісу Gateway.

Виконання вимоги надання змістовної звітової інформації було виконано в мікросервісі Logger. Даний мікросервіс надає мінімальні можливості для користувача, а саме вивід звітової інформації. Таке рішення було прийнято в цілях полегшення роботи з системою захисту та тим, що система буде захищати від атак типу XSS та SQL Injection без збоїв.

3.2 Реалізація системи захисту інформації в корпоративній мережі

Передумовами для розгортання системи захисту є операційна система Windows, Linux, macO або в Docker на робочій станції або сервері, який топологічно розташований перед захищуваною мережею.

3.2.1 Визначення та опис компонентів системи

Для початку потрібно створити структуру системи захисту, описати її компоненти та план взаємодії компонентів. Для даної системи вирішено розробити програмний пакет за допомогою технології ASP.NET Core. Програмний пакет складатиметься з чотирьох взаємодіючих між собою компонентів. Для цього архітектура додатку реалізовуватиметься за допомогою патерну «мікросервісної архітектури».

Як вже було визначено система захисту буде складатися з чотирьох компонентів захисту:

1. Gateway на основі реверсивного проксі-сервера.
2. Firewall (Брандмауер).
3. Logger.
4. DigitalSignatureVerifier.

Та елементів, які дозволять протестувати систему захисту як цілісну імітаційну модель:

1. Internet.
2. Kali Linux.
3. Corporate Network (власне захищувана корпоративна мережа).

Опишемо детальніше кожен з компонентів, його мету, функції та складемо структурну схему та діаграми:

- послідовності;
- компонентів;
- розгортання.

Розпочнемо з загального вигляду робочої системи, його зображення наведено у графічному матеріалі.

Перечислимо та опишемо детальніше кожен елемент системи захисту, його роль, функції та реалізацію. Опис функції програмного коду наведений в розділі «Специфікація функцій».

3.2.1.1 Елемент системи Internet

Компонент системи Internet, буде грати одну з найважливіших ролей в нашій системі захисту інформації, так як саме з цього елементу під час симуляції імітаційної моделі в GNS3 будуть намагатися пройти, згенеровані за допомогою програмного пакету Kali Linux, загрози в нашу корпоративну мережу. Компонент Internet відіграватиме роль зловмисника, атакуючого корпоративну мережу.

Функції даного елементу системи захисту зрозумілі, генерація загроз та спроби надсилання загроз на endpoint-и корпоративної мережі.

Реалізація даного компоненту буде взята з готового програмного пакету в Kali Linux. Для імітації атакуючої сторони було обрано програму Vega Usage. Дана програма буде імітувати загрози наступних типів:

1. XSS (Cross Site Scripting);
2. SQL Injection.

3.2.1.2 Елемент системи Kali Linux

Даний елемент виконуватиме роль генератора загроз обраних типів. Для більшої зрозумілості опис можливих загроз для корпоративної мережі наведено в розділі 2 Огляд предметної області.

В даній дипломні роботі буде проведено стрес-тестування розробленої системи захисту за допомогою програми Vega Usage, яка буде генерувати загрози (XSS, SQL Injection).

3.2.1.3 Елемент системи захисту Gateway

Даний елемент, розроблений з використанням reverse-proxy програмного дизайну, буде виконувати роль реверсивного проксі-серверу, який буде перенап-

равляти запити на endpoint-и корпоративної мережі.

Реверсивний проксі-сервер - це сервер, який розташований перед веб-серверами і пересилає клієнтські (наприклад, веб-браузер) запити до цих веб-серверів. Зворотні проксі, як правило, реалізуються для підвищення безпеки, продуктивності та надійності. Щоб краще зрозуміти, як працює зворотний проксі і які його переваги, давайте спочатку визначимо, що таке проксі-сервер.

Проксі-сервер, є сервером, який знаходиться перед групою клієнтських машин. Коли ці комп'ютери надсилають запити на сайти та послуги в Інтернеті, проксі-сервер перехоплює ці запити, а потім спілкується з веб-серверами від імені тих клієнтів, як посередник. Дану модель можна розглянути на рисунку 14 [10].

Наприклад, визначимо 3 комп'ютери, які беруть участь у типовій передачі проксі-проксі:

A: Це домашній комп'ютер користувача (user’s device);

B: Це проксі-сервер (forward-proxy);

C: Це сервер-джерело, де зберігаються дані веб-сайту (origin server).

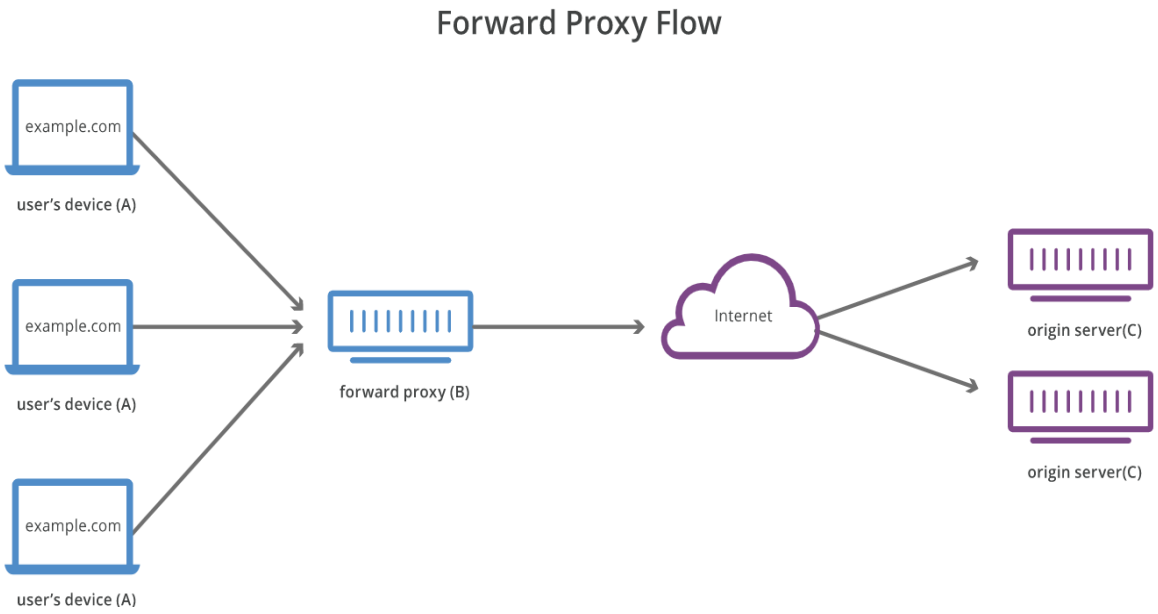

Рисунок 14 – Проходження запиту на сервер-джерело через проксі-сервер

У стандартному інтернет-зв'язку комп'ютер А досягає безпосередньо до

комп'ютера C, при цьому клієнт надсилає запити на сервер-джерело що відповідає клієнту. Коли проксі-сервер знаходиться на місці, A замість цього надсилатиме запити до B, які потім пересилатимуть запит до C. C потім надсилатиме відповідь B, який пересилатиме відповідь на A.

Реверсивний проксі-сервер - це сервер, який знаходиться перед одним або декількома веб-серверами, перехоплюючи запити від клієнтів. Він відрізняється від проксі-сервер, де проксі-сервер знаходиться перед клієнтами. З реверсивним проксі-сервером, коли клієнти надсилають запити на сервер-джерело, ці запити перехоплюються на межі мережі за допомогою реверсивного проксі-сервера. Потім сервер реверсивного проксі-сервера надсилатиме запити до сервера початкового сервера та отримувати відповіді.

Різниця між прямим і реверсивним проксі ледь помітна, але важлива. Підсумовуючи це можна сказати про те, що проксі-сервер стоїть перед клієнтом і гарантує, що жоден сервер-джерело ніколи не спілкується безпосередньо з конкретним клієнтом. З іншого боку, реверсивний проксі-сервер розташований перед сервером-джерелом і гарантує, що жоден клієнт не зв'язується безпосередньо з цим сервером.

Ще раз проілюструємо, на рисунку 15 [10], назвавши комп'ютери:

D: Будь-яка кількість домашніх комп'ютерів користувачів

E: Це зворотний проксі-сервер

F: Один або більше серверів походження

Функціями Gateway будуть розпізнавання та трактування web-запиту до одного з endpoint-ів, фільтрація нерозпізнаних, некоректних чи з загрозливим вмістом запитів на endpoint-и корпоративної мережі.

Опис алгоритму роботи даного компоненту можна розглянути на рисунку 16.

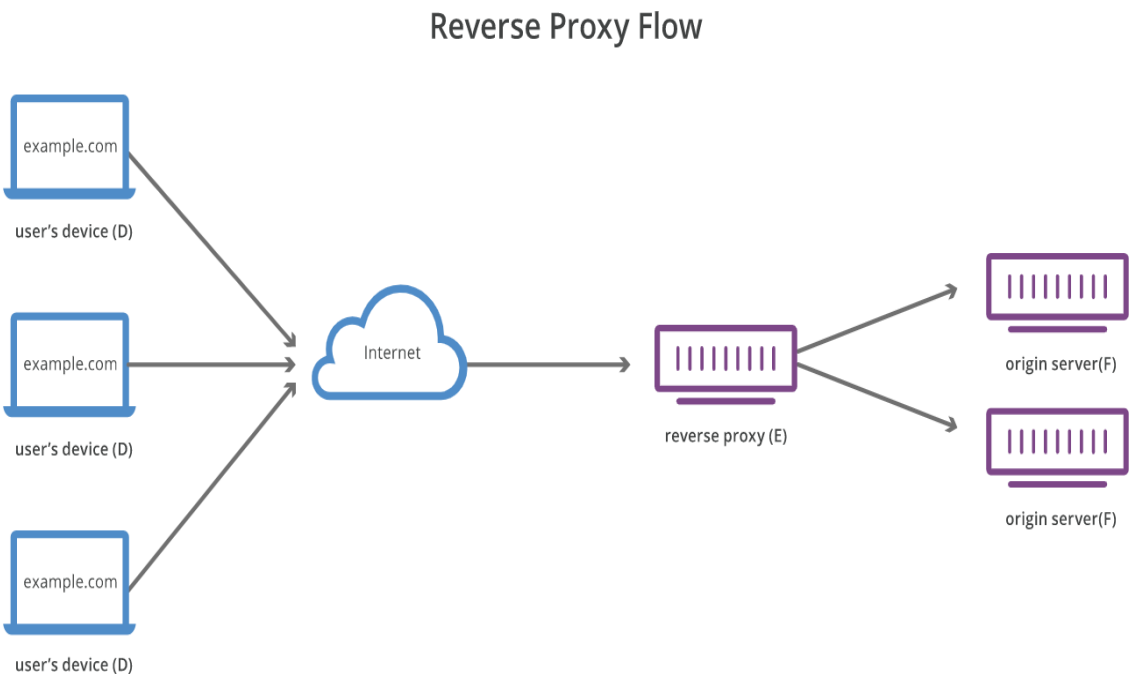

Рисунок 15 - Проходження запиту на сервер-джерело через реверсивний проксі-сервер

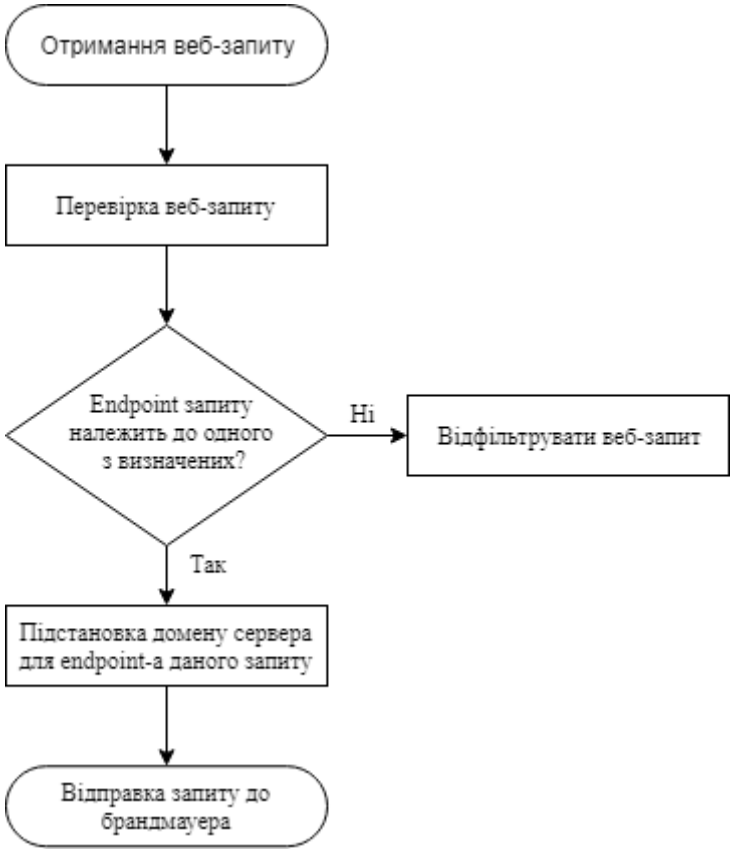

Рисунок 16 - Алгоритм роботи Gateway елементу системи захисту

Структура проекту програмної реалізації Gateway компонента системи захисту наведено на рисунку 18:

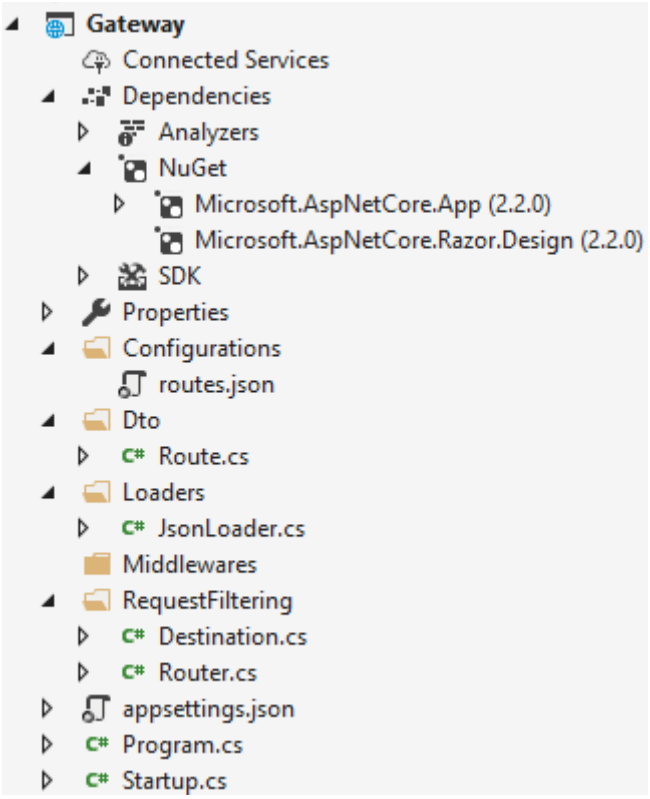

Рисунок 17 - Структура проекту програмної реалізації Gateway компонента системи захисту

3.2.1.4 Елемент системи захисту Firewall (Брандмауер)

Загальні відомості про те, що таке Брандмауер, його основні функції наведено в розділі 2.5 «Брандмауер». Зараз опишемо роль брандмауера в нашій систем та функції, які він буде виконувати.

Основна роль Брандмауера буде заключатися в фільтрації web-запитів, які пройшли відсіювання на етапі проходження крізь Gateway. Прикладом такої ситуації може бути ситуація, коли зловмисник або хакер, заздалегідь знає про структуру запитів на endpoint-и корпоративної мережі або ж методом викрадення чи підслуховування заволодів URL-и, якими можна відтворювати запити до корпоративної мережі. Також такою інфор-

мацією зловмисник може заволодіти маючи інсайдера, працівника корпоративної мережі [11].

Функціями Брандмауера буде відсіювання зловмисних, підозрілих або з підозрілим вмістом запитів, перевіркою електронно-цифрового підпису, за допомогою мікросервісу DigitalSignatureVerifier.

Опис алгоритму роботи даного компоненту можна розглянути на рисунку 19:

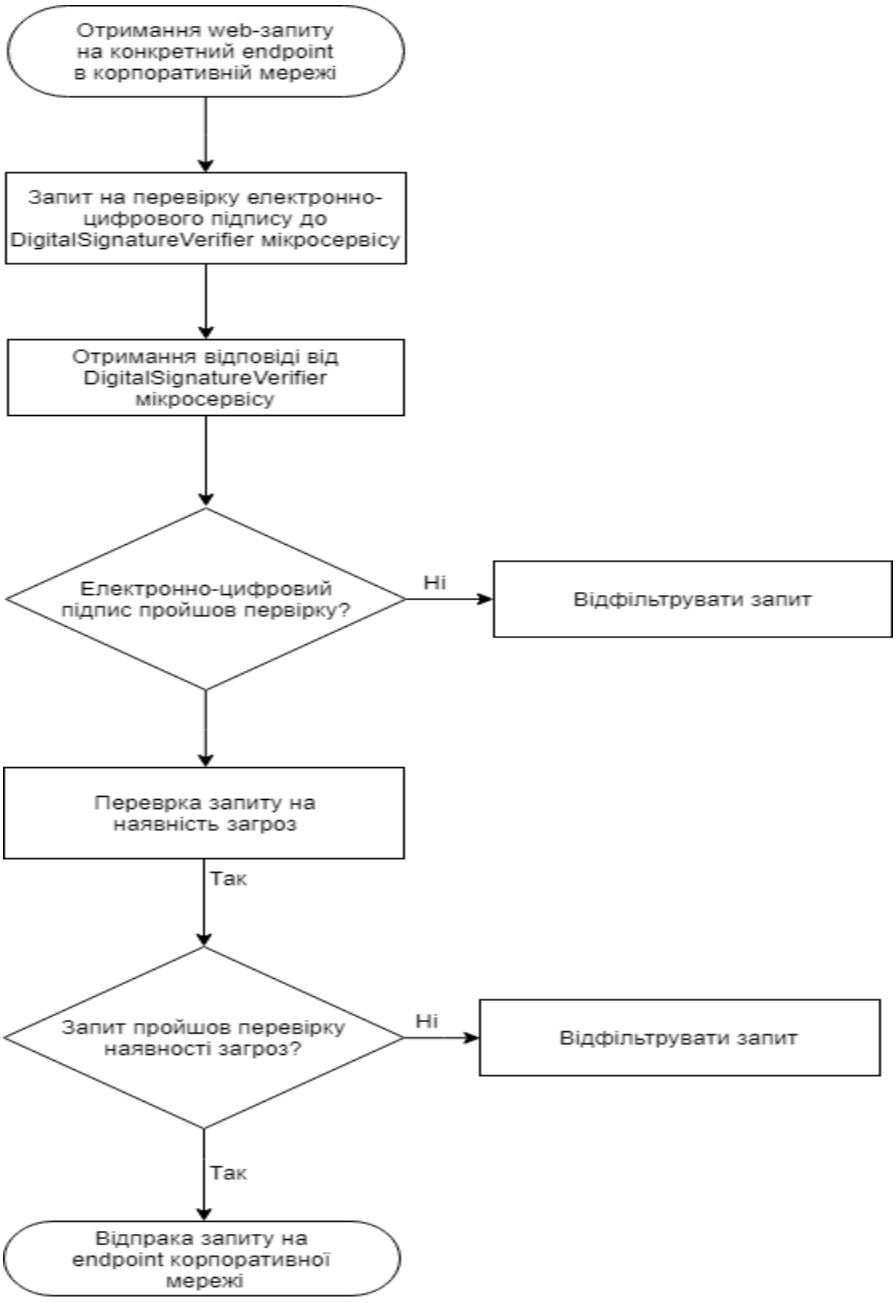

Рисунок 18 - Алгоритм роботи Firewall елементу системи захисту

Структура проекту програмної реалізації Firewall компонента системи захисту наведено на рисунку 20:

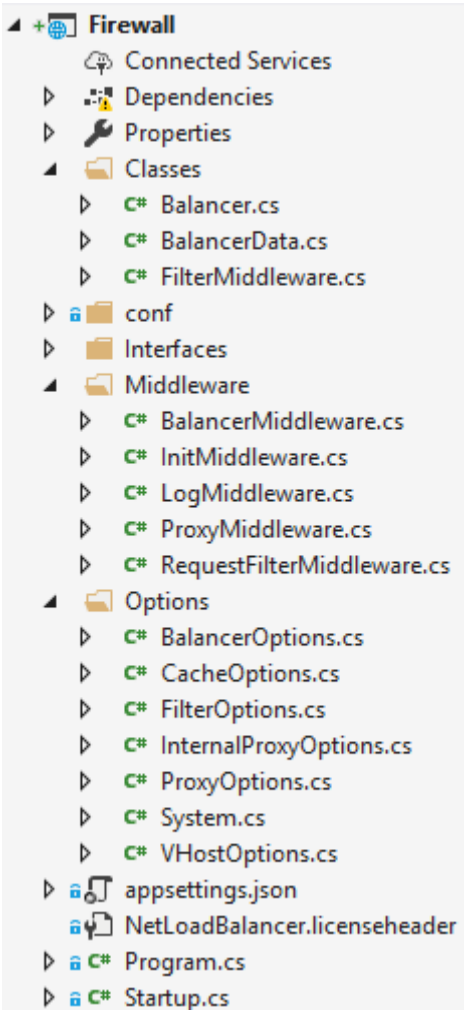

Рисунок 19 - Структура проекту програмної реалізації Firewall компонента системи захисту

3.2.1.5 Елемент системи захисту DigitalSignatureVerifier

Загальні відомості про те, що таке електронно-цифровий підпис, його основні функції, призначення та принцип дії наведено в розділі «Електронно-цифровий підпис». Зараз опишемо роль верифікатора електронно-цифрових ключів в нашій системі та функції, які він буде виконувати.

Роль верифікатора буде полягати в підтвердженні або спростуванні права

проходження для web-запиту у корпоративну мережу [12].

Основними функціями буде перевірка прийнятих електронно-цифрових підписів з базою створених підписів, відправка спростування або підтвердження підпису на Брандмауер, створення та зберігання в базу нових електронних підписів.

Опис алгоритму роботи даного компоненту під час запиту на перевірку електронно-цифрового підпису можна розглянути на рисунку 21:

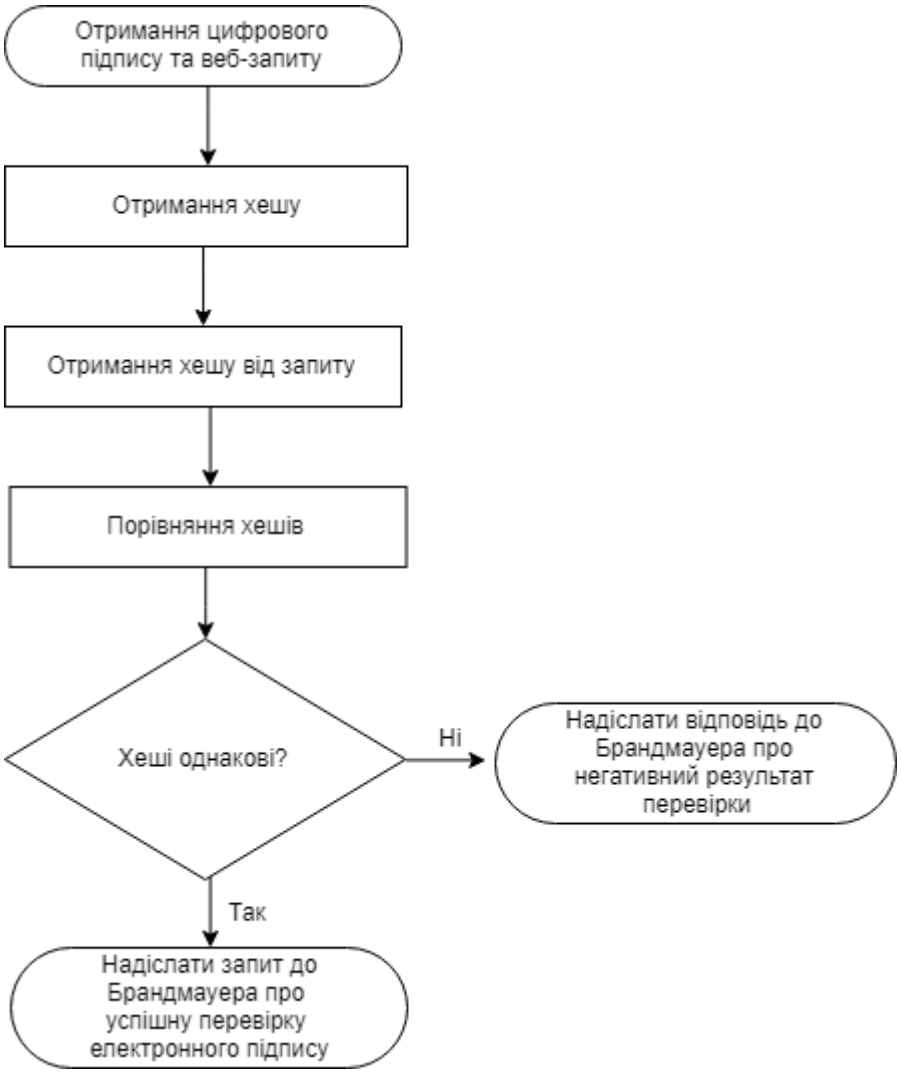

Рисунок 20 – Алгоритм роботи DigitalSignatureVerifier під час запиту на перевірку цифрового підпису

Структура проекту програмної реалізації DigitalSignatureVerifier компонента системи захисту наведено на рисунку 21:

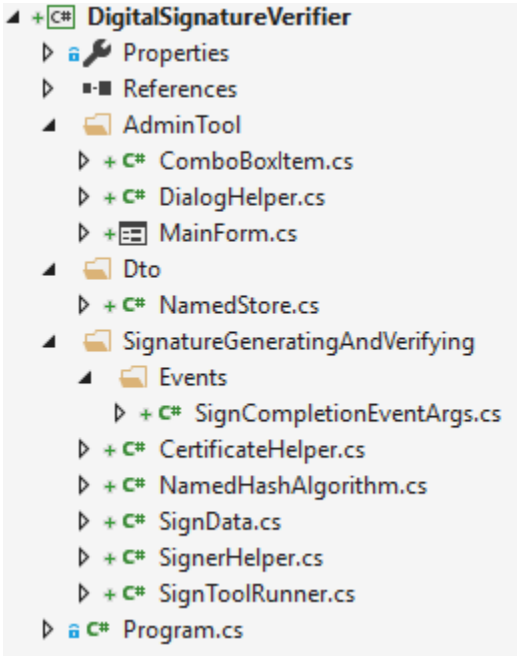

Рисунок 21 - Структура проекту програмної реалізації DigitalSignatureVerifier компонента системи захисту

3.2.1.6 Алгоритм формування електронно-цифрового підпису

В даній дипломній роботі було прийнято рішення використання цифрового підпису для підсилення системи захисту корпоративної мережі від проникнення зловмисних web-запитів.

Зазвичай вистачає використання таких методів захисту як:

- Перевірка вводу користувача.
- Автентифікація та авторизація.
- Парсинг вмісту web-запиту.
- Використання throttling методів від перевантаження серверу.

Але існує не мала ймовірність, що зловмисник матиме інсайдера в корпоративній мережі або зловмисним чином викраде ключі чи паролі аутентифікації або знатиме як запакувати вміст запиту таким чином, щоб обійти захисний парсинг вмісту запиту. В такому разі одним з кращих, на останніх етапах, захисної системи, методів захисту буде перевірка електронно-цифрового підпису [13].

Отже, тепер детальніше розберемо сам алгоритм формування цифрового підпису та його перевірку при надходженні запиту на мікросервіс DigitalSignatureVerifier. Програмний код алгоритму наведено у додатках.

Електронно-цифровий підпис зі скороченим розміром підпису, у практичному використанні повинні забезпечуватися стійкістю необхідного рівня. Довжина підпису зі скороченим розміром має приблизно однакову довжину з DSS та ГОСТ Р 34.10-94. Якщо рівень підробки підпису буде складати приблизно 2^{80} операцій зведення в степінь за модулем, тоді розмір такого підпису буде дорівнювати 320 бітам.

В даному алгоритмі приватний ключ γ, буде складати порядок групи, яка буде генеруватися числом α, та повинен бути збільшеним удвічі в порівнянні з розміром, достатнім для присікання атак на основі вгадування значень γ або на основі повного перебору. Дана ситуація зв'язана з тим, що γ повинен бути складним і утримувати в якості свої співмножників, у крайньому випадку, по одному великому множнику на розкладений член r-1 і q-1, тобто γ= γ' γ'', де у'|r-1 та у''|q-1. Для розкладання числа n з використанням відомого значення α, може бути взято обчислення найбільшого загального дільника чисел n і (α^i modn)-1. В цьому способі факторизації методом послідовного перебору потрібно знайти таке значення i_0, при якому виконується співвідношення НСД (α^i modn -1, n)≠1 (в такому випадку НСД дорівнюватиме r, або q). Якщо задається рівень стійкості приблизно 2^{80} операцій, то довжина кожного з чисел γ' і γ'' повинна дорівнювати 80 бітам, тобто маємо | γ |≈160 біт. Таким чином елементи підпису (k, g) обчислюються по 160-бітовому модулю, що визначає розмір підпису, рівний 320 біт. Особливістю схем з відкритим ключем типу (α, n) є те, що подвоєння розміру елементів підпису пов'язано з атаками, використовують параметр αдля факторизації модуля n. Інший спосіб усунення можливості розкладання модуля n в'язати з використанням простого значення γ, такого що γ |r -1 і γ |q -1, проте в цьому випадку секретне значення γ може бути знайдено як дільник числа n-1 [14].

Конкретний варіант реалізації схеми з 160-бітовими елементами підпису

(k, g) представлений нижче.

Рішення для перевірки обчислюється за формулою:

$$k - g = (\alpha^{\beta^{kgH} mod n} mod p) mod \delta \quad (3.1)$$

де операція modδ грає роль зжимаючої функції. Обчислення підпису виконується на основі рішення наступної системи відношень:

$$\begin{cases} k - g = Z \\ kgH \equiv U mod \gamma \end{cases} \quad (3.2)$$

в якій значення U < γ вибирається випадково, а значення Z обчислюється за формулою . Рішення системи дає наступні формули для обчислення елементів підпису:

$$g = -\frac{Z}{2} \pm \sqrt{\frac{Z^2}{4} + \frac{U}{H}} mod \gamma \text{ та } k = Z + g \quad (3.3)$$

Алгоритм ідентифікації підпису потрібен для перевірки факту незмінності передаваного запиту. Під час ідентифікації, проводиться перевірка хеш-суми: якщо будь який сертифікат не відповідає своєму декриптованому за допомогою алгоритму хешування двійнику – система сповістить про це в мікросервіс Logger і передасть команду відповідь до Брандмауера про негативний результат ідентифікації. Розглянемо даний алгоритм детальніше на рисунку 22.

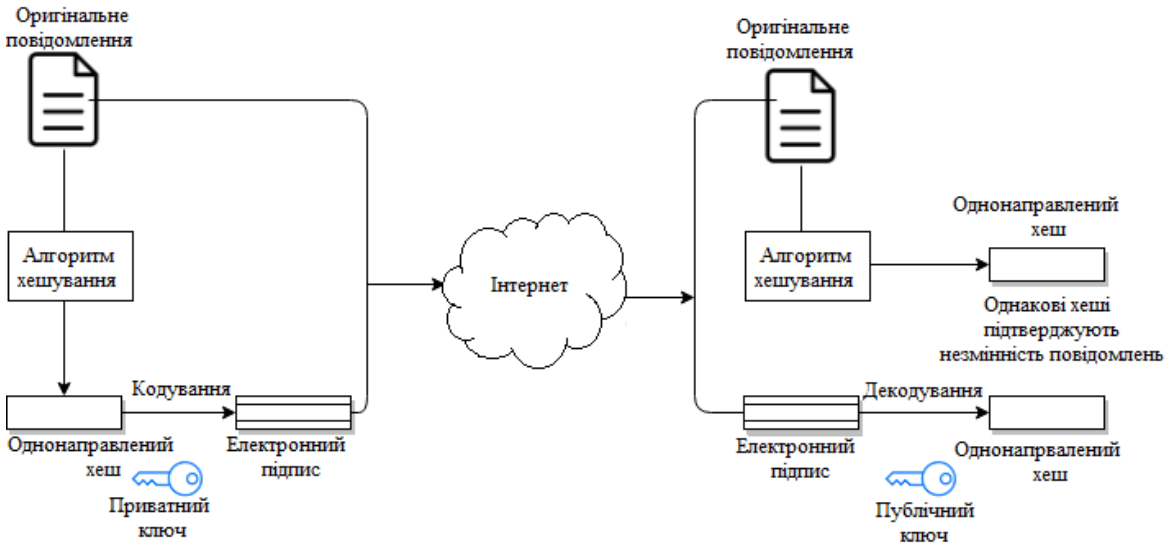

Рисунок 22 – Алгоритм роботи електронно-цифрового ключа

1. Дайджест повідомлення обчислюється шляхом застосування хеш-функції на повідомленні, а потім дайджест повідомлення зашифровується за допомогою приватного ключа відправника для формування цифрового підпису. (Цифровий підпис = Кодування(приватний ключ відправника, дайджест повідомлення) і дайджест повідомлення = алгоритм збору повідомлення (повідомлення)).

2. Потім з повідомленням передається цифровий підпис (передається повідомлення + електронний підпис);

3. Приймач розшифровує цифровий підпис за допомогою відкритого ключа відправника (це гарантує автентичність, оскільки лише відправник має свій закритий ключ, так що лише відправник може зашифрувати свій закритий ключ, який може бути розшифровано відкритим ключем відправника);

4. Приймач тепер має дайджест повідомлення;

5. Приймач може обчислити дайджест повідомлення з повідомлення (фактичне повідомлення надсилається з цифровим підписом);

6. Дайджест повідомлень, обчислений приймачем і дайджест повідомлення (отриманий шляхом розшифрування цифрового підпису), повинен бути однаковим для забезпечення цілісності.

3.2.1.7 Елемент системи захисту Logger

Останнім і не менш головним компонентом системи захисту є мікросервіс логування. Основна роль даного елементу є запис усіх дій що відбуваються під час надходження та проходження веб-запиту крізь систему захисту. Цей мікросервіс надасть можливість переглядати інформацію стосовно прийнятого запиту та всіма діями або заходами, якщо це виявився загрозливий запит, які були застосовані для його подальшого проходження до корпоративної мережі. Або заходи для фільтрації даного запиту, якщо він становив загрозу для корпоративної

мережі.

Основними функціями даного компоненту є запис (логування) усіх дій над запитом, конвертаціями, читанням та фільтрацією запитів, які надходять з мережі Інтернет в систему захисту. Логер дозволить зібрати статистику та проаналізувати продуктивність та результатовіддачу розробленої системи захисту. Аналіз потужності захисту дозволить в подальшому виділити слабкі місця захисту та зпростить виділення умов для розробки покращень.

Алгоритм роботи даного компоненту дуже простий і не потребує візуального зображення, діаграм чи схем. Опис алгоритму не потрібен, тому що даний мікросервіс являється додатком типу Web API і буде приймати запити на логування від інших мікросервісів системи захисту.

Структура проекту програмної реалізації Logger компонента системи захисту наведено на рисунок 23:

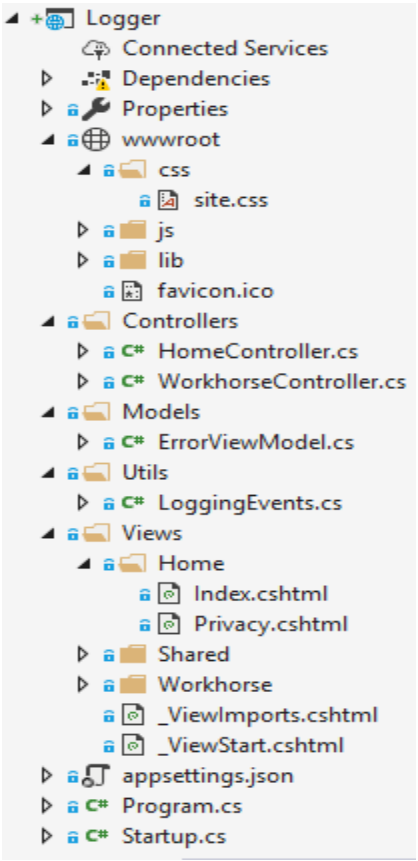

Рисунок 23 - Структура проекту програмної реалізації Logger компонента системи захисту

3.3 Конфігурація Kali Linux

Перш ніж будувати імітаційну схему в GNS3, потрібно подбати про вибір програмного віджета, який буде симулювати атаки на корпоративну мережу. Для даної дипломної роботи, для виконання цілей атакуючої сторони, було обрано програмний операційну систему Kali Linux, вона містить широкий спектр програм та віджетів для зловмисних атак.

Kali Linux є одним з кращих пакунків безпеки з відкритим кодом хакера, що містить набір інструментів, розділений за категоріями. Kali Linux може бути встановлений на машині як операційна система. Встановлення Kali Linux є практичним варіантом, оскільки надає більше можливостей для роботи та поєднання інструментів.

Як правило, Kali Linux може бути встановлений на машині як операційна система, як віртуальна машина. Встановлення Kali Linux є практичним варіантом, оскільки надає більше можливостей для роботи та поєднання інструментів.

Завантажимо та встановимо Virtual Box. Virtual Box особливо корисний, коли ви хочете перевірити щось на Kali Linux. Запуск Kali Linux на віртуальному вікні безпечний, якщо ви хочете експериментувати з невідомими пакунками або коли ви хочете протестувати код.

За допомогою Virtual Box можна встановити Kali Linux в систему (а не безпосередньо на жорсткому диску) поряд з основною ОС. Після встановлення Virtual Box, потрібно встановити Kali Linux на віртуальну машину.

В нашому випадку потрібно створити три хости в Virtual Box:

1. Хост Kali Linux.
2. Хост ПК на якому буде запущена система захисту.
3. Хост Ubuntu зі встановленим GNS3.

Хост Kali Linux потрібен для того, щоб під’єднати його за допомогою інструментів віртуальної машини в середину топології, яка буде побудована в GNS3. На даному хості буде встановлена Kali Linux операційна система, на ній

буде запущено програмний пакет Vega Usage.

Vega Usage є безкоштовним сканером і тестовою платформою з відкритим кодом для перевірки безпеки веб-додатків. Vega може допомогти вам знайти та перевірити SQL Injection, Cross-Site Scripting (XSS), ненавмисно розкривши конфіденційну інформацію та інші уразливості. Він написаний на Java, заснований на графічному інтерфейсі і працює на Linux, OS X і Windows.

Vega включає в себе автоматизований сканер для швидких тестів і перехоплюючий проксі для тактичної перевірки. Vega може бути розширена за допомогою потужного API на мові веб: JavaScript.

Хост ПК на якому буде задеплоєна система захисту потрібен для розгортання прошарку захисту в нашій системі. Сконфігурований хост буде підключено в середину GNS3 і він буде відігравати роль проксі-сервера, через якого веб запити прямуватимуть до корпоративної мережі.

І остання віртуальна машина з хостом з операційною системою Ubuntu на борту відіграватиме роль тестового середовища. В середині GNS3 буде побудована топологія нашої системи. Структурну схему всієї системи можна розглянути в додатках.

3.3.1 Конфігурація Kali Linux Vega Usage

Для того щоб встановити додаток Vega потрібно запустити наступну команду в терміналі Kali Linux:

apt-get update && apt-get install -y vega

після встановлення Vega буде доступна для запуску як на рисунку 24.

Рисунок 24 – Vega доступна в улюблених додатках Kali Linux

Після встановлення Vega не потребує додаткових конфігурацій, окрім вибору потрібних інструментів взлому, отже при налаштуванні Vega як на рисунку 25 потрібно обрати як мінімум XSS та SQL Injection типи загроз.

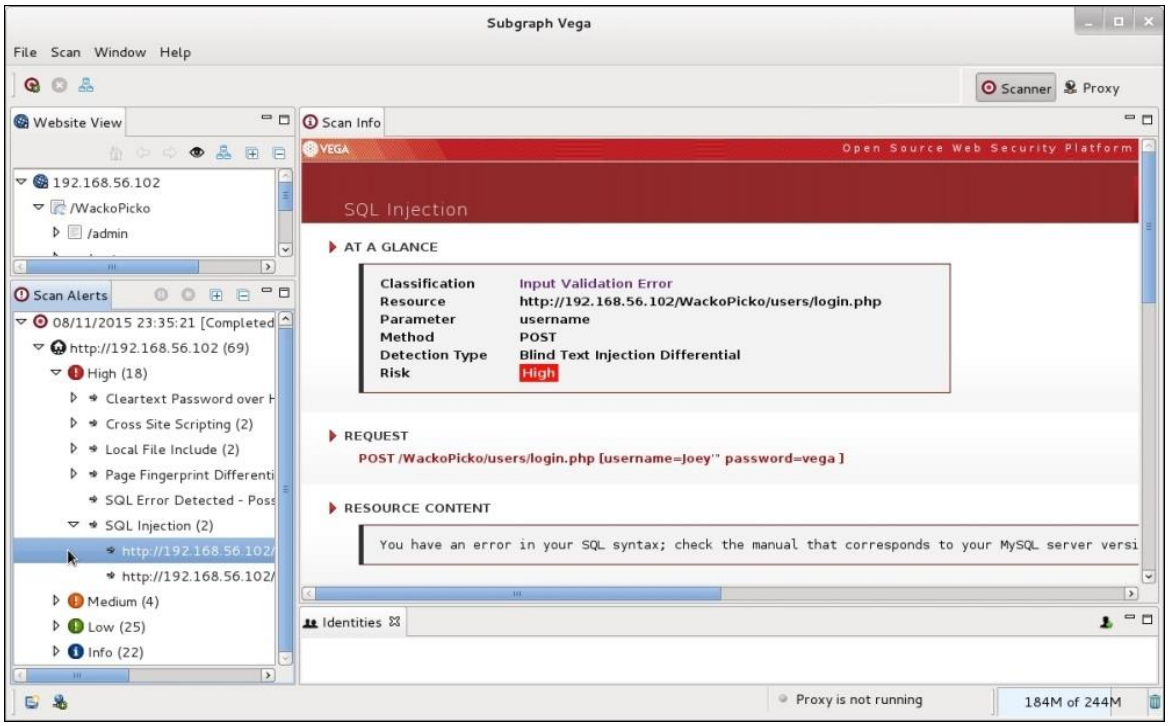

Рисунок 25 - Додаток Vega в запущеному стані

3.4 Налаштування GNS3

Для розгортання та симуляції даної імітаційної моделі було обрано GNS3. Після завершення симуляції будуть представлені результати тестування, які до-

зволить проаналізувати якість розробленої системи захисту.

3.4.1 Основні відомості про GNS3

GNS3 використовується сотнями тисяч мережевих інженерів по всьому світу для емуляції, налаштування, тестування та усунення несправностей віртуальних і реальних мереж. GNS3 дозволяє запускати невелику топологію, що складається лише з декількох пристроїв на вашому ноутбуці, до тих, які мають багато пристроїв, розміщених на декількох серверах або навіть розміщених у хмарі. GNS3 - вільне програмне забезпечення з відкритим вихідним кодом. Він активно розвивається і підтримується і має зростаюче співтовариство понад 800 000 членів. GNS3 дозволяє мережевим інженерам віртуалізувати реальні апаратні пристрої вже більше 10 років. Спочатку тільки емуляція Cisco пристроїв з використанням програмного забезпечення під назвою Dynamips, GNS3 тепер еволюціонував і підтримує багато пристроїв від декількох постачальників мережі, включаючи Cisco віртуальні комутатори, Cisco ASA, Brocade vRouters, Cumulus Linux комутатори, Docker екземпляри, HPE VSR, кілька пристроїв Linux і багато інших.

3.4.2 Архітектура GNS3

GNS3 складається з двох програмних компонентів:

1. Програмне забезпечення GNS3-все-в-одному (GUI)
2. Віртуальна машина GNS3 (VM)

GNS3-все-в-одному:

Це клієнтська частина GNS3 і є графічним інтерфейсом користувача (GUI). Ви встановлюєте програмне забезпечення «все-в-одному» на локальному комп'ютері (Windows, MAC, Linux) і створюйте свої топології за допомогою цього програмного забезпечення. Приклад побудованої топології можна розгля-

нути на наступному рисунку 26:

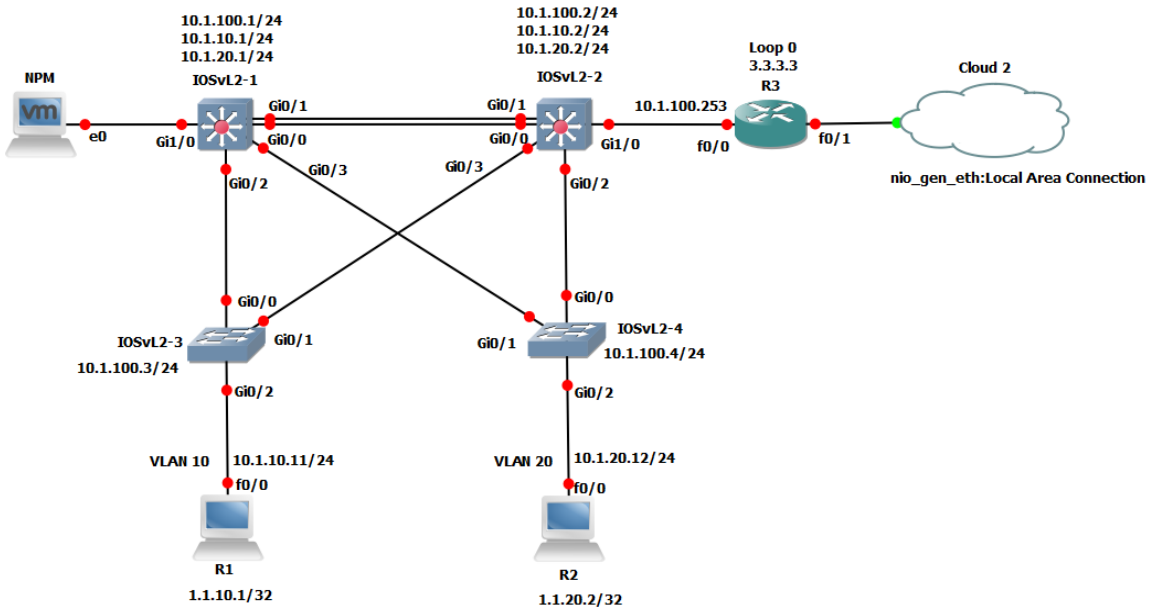

Рисунок 26 – Приклад побудованої топології в GNS3-все-в-одному

Параметри сервера. Коли ви створюєте топології в GNS3, використовуючи клієнт програмного графічного інтерфейсу «все-в-одному», створені пристрої повинні бути розміщені і запускатися сервером. У вас є кілька варіантів для серверної частини програмного забезпечення:

- Локальний сервер GNS3;
- Локальний GNS3 VM;
- Дистанційне керування GNS3 VM.

Локальний сервер GNS3 працює локально на тому ж ПК, де встановлено програмне забезпечення GNS3 all-in-one. Якщо, наприклад, ви використовуєте ПК з ОС Windows, як GNS3 GUI, так і локальний сервер GNS3 працюють як процеси в Windows. Додаткові процеси, такі як Dynamips, також працюватимуть на вашому ПК.

Якщо було вирішено використовувати GNS3 VM, можна або запустити GNS3 VM локально на вашому комп'ютері за допомогою програм віртуалізації, таких як VMware Workstation або Virtualbox; або можна запустити віртуальну машину GNS3 дистанційно на сервері за допомогою VMware ESXi або навіть у

хмарі.

Можна використовувати GNS3 без використання GNS3 VM. Це хороший спосіб розпочати роботу спочатку, але ця установка обмежена і не надає стільки варіантів, що стосуються розміру топології та підтримуваних пристроїв. Якщо потрібно створити більш просунуті топології GNS3 або включити такі пристрої, як пристрої Cisco VIRL (IOSvL2, IOSvL3, ASAv) або інші пристрої, які потребують Qemu, рекомендується GNU3 VM.

GNS3 підтримує як емульовані, так і імітовані пристрої. Емуляція GNS3 імітує або емулює апаратні засоби пристрою, а фактичні зображення виконуються на віртуальному пристрої. Наприклад, можна скопіювати Cisco IOS з реального, фізичного маршрутизатора Cisco і запустити його на віртуальному, емульованому маршрутизаторі Cisco в GNS3. Симулювання GNS3 імітує функції та функціональні можливості такого пристрою, як комутатор. Ви не запускаєте реальні операційні системи, такі як Cisco IOS, а скоріше моделюється пристрій, розроблений GNS3, наприклад, перемикач 2 рівня GNS3.

Різниця між емуляцією та симуляцією:

1. Dynamips - це старіша технологія, що імітує обладнання Cisco. Він використовує реальні зображення Cisco IOS. Це добре для базових топологій типу CCNA, але має ряд обмежень, таких як підтримка старих версій Cisco IOS (12.X), які також не підтримуються або активно оновлюються Cisco.

2. Рекомендовані зображення Cisco для використання з GNS3 - це зображення з Cisco VIRL (IOSv, IOSvL2, IOS-XRv, ASAv). Ці зображення підтримуються та активно оновлюються компанією Cisco. Зображення підтримують поточні випуски Cisco IOS (15.X) і забезпечують найкращий масштаб і досвід користувачів.

3.4.3 Переваги та недоліки GNS3

Як вже згадувалося, GNS3 - це програмне забезпечення з відкритим вихід-

ним кодом, яке можна завантажити і використовувати безкоштовно. Вихідний код доступний на GitHub.

1. Переваги:

- вільне програмне забезпечення;
- програмне забезпечення з відкритим вихідним кодом;
- ні щомісячних або щорічних ліцензійних платежів;
- немає обмежень щодо кількості підтримуваних пристроїв (лише обмеження - це ваше обладнання: процесор і пам'ять);
- підтримує декілька варіантів перемикання (ESW16 Etherswitch, IOU / IOL Layer 2 зображення, VIRL IOSvL2);
- підтримує всі зображення VIRL (IOSv, IOSvL2, IOS-XRv, CSR1000v, NX-OSv, ASAv);
- підтримка кількох середовищ постачальників;
- може працювати з гіпервізорами або без них;
- підтримує як безкоштовні, так і платні гіпервізори (Virtualbox, робоча станція VMware, програвач VMware, ESXi, Fusion);
- доступні для завантаження, безкоштовні, попередньо налаштовані та оптимізовані пристрої для спрощення розгортання;
- рідна підтримка Linux без необхідності в додатковому програмному забезпеченні віртуалізації;
- програмне забезпечення від декількох постачальників вільно доступні;
- велика та активна спільнота (800 000 користувачів).

2. Недоліки:

- зображення Cisco потрібно надіслати користувачем (завантажити з Cisco.com або придбати ліцензію VIRL або скопіювати з фізичного пристрою);
- не є автономним пакетом, але вимагає локальної установки програмного забезпечення (GUI);

- на GNS3 можуть вплинути налаштування та обмеження вашого комп'ютера через локальну інсталяцію (брандмауер та налаштування безпеки, правила корпоративного ноутбука тощо).

3.4.4 Встановлення та конфігурація GNS3

В даній дипломній роботі буде використано операційну систему Linux. Тому наступна інструкція по встановленню та конфігурації буде специфічна саме для даної ОС.

Для встановлення GNS3 на персональний комп’ютер потрібно ввести та запустити наступні команди в terminal-і Linux-а:

sudo add-apt-repository ppa:gns3/ppa

sudo apt-get update

sudo apt-get install gns3-gui

Далі відкриваємо щойно встановлений GNS3 та розпочнемо конфігурацію. Майстер налаштування GNS3 відображається як на рисунку 27, коли GNS3 запускається вперше. Це забезпечує простий спосіб налаштування параметрів GNS3:

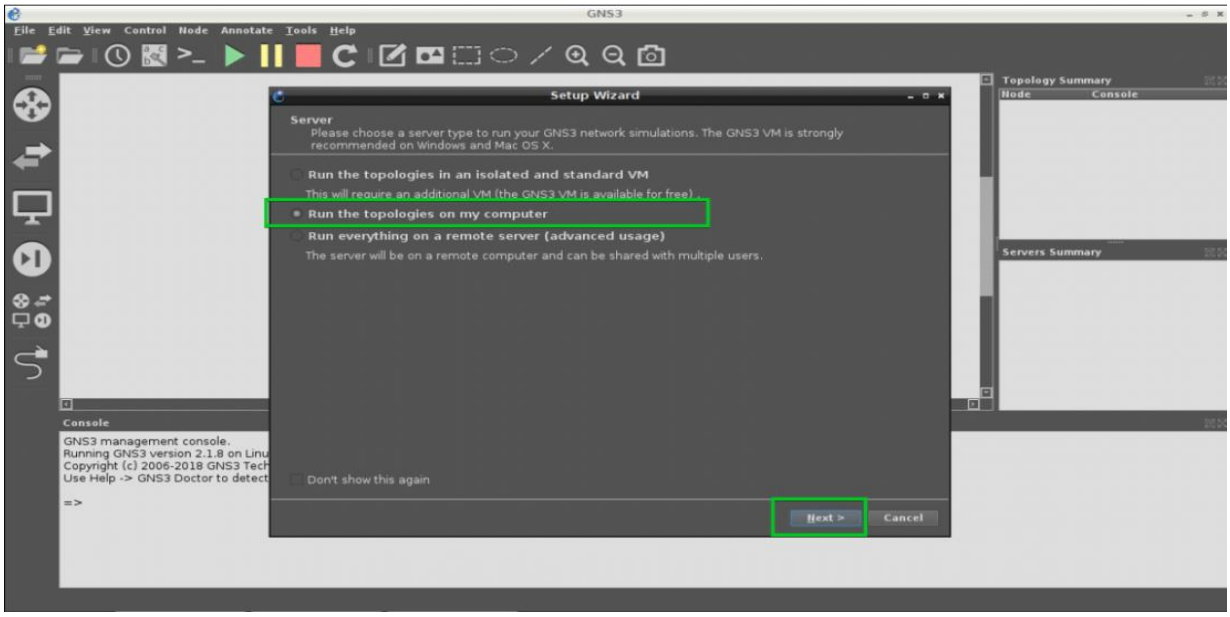

Рисунок 27 – Майстер початкового налаштування GNS3

Вибираємо пункт “Run topologies on my computer”, даний вибір означатиме, що ми запускатимемо усі налаштовані топології на нашому ПК.

Конфігурацію локального серверу залишимо такою як на рисунку 28:

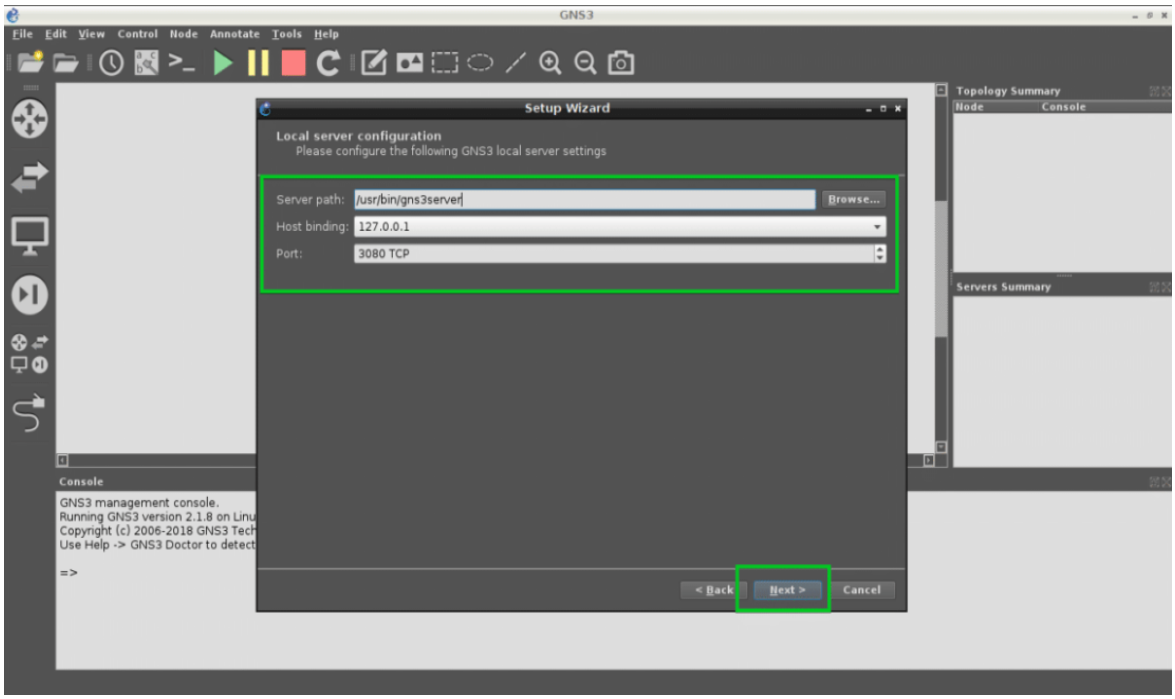

Рисунок 28 - Налаштування локального серверу

Далі пропускаємо всі кроки. Налаштування GNS3 майже закінчено, лишилось додати компоненти в імітаційну модель, побудувати невелику корпоративну мережу та встановити елемент Kali Linux.

Для симуляції імітаційної моделі потрібно підключити два Virtual Box хости. На першому розгорнута операційна система Windows та запущена система захисту. На другому розгорнута операційна система Kali Linux та Vega додаток.

Підключення першого хосту почнемо з додавання хосту в GNS3. Перейдемо в Edit -> Preferences. Виберемо пункт VirtualBox VMs як на рисунку 29.

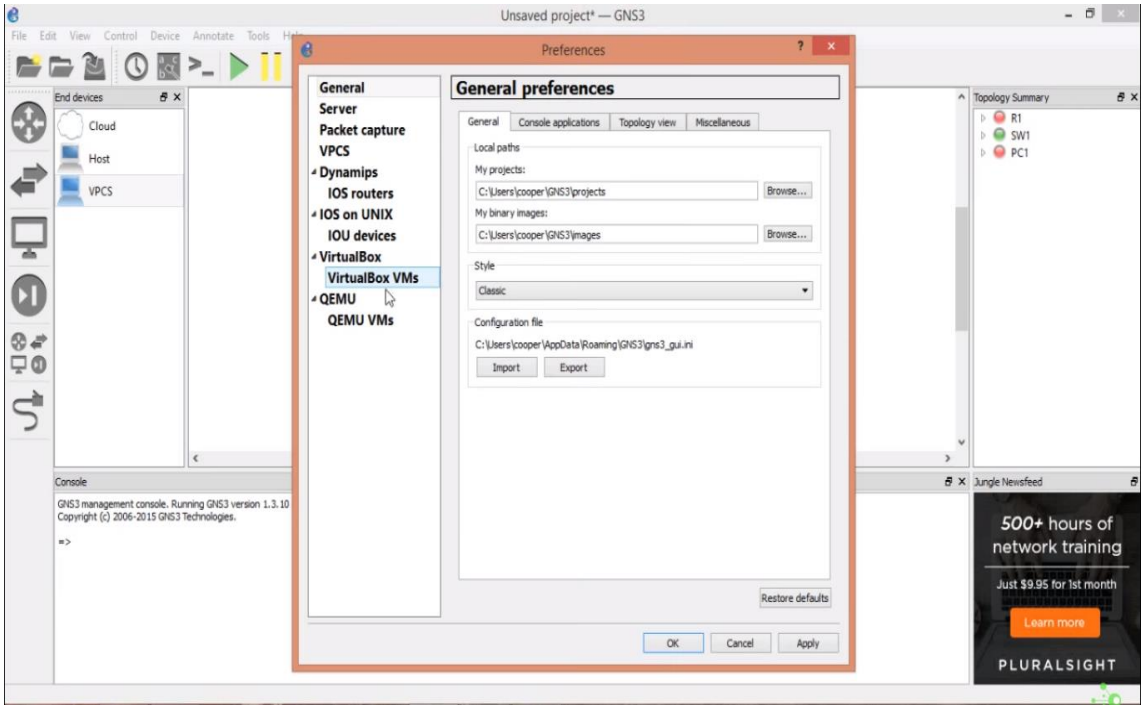

Рисунок 29 – Вікно Preferences

Натискаємо створити нову, після чого з’являється вікно підключення вже створених віртуальних машин. Вибираємо віртуальну машину з розгорнутою на ній системою захисту якна рисунку 30.

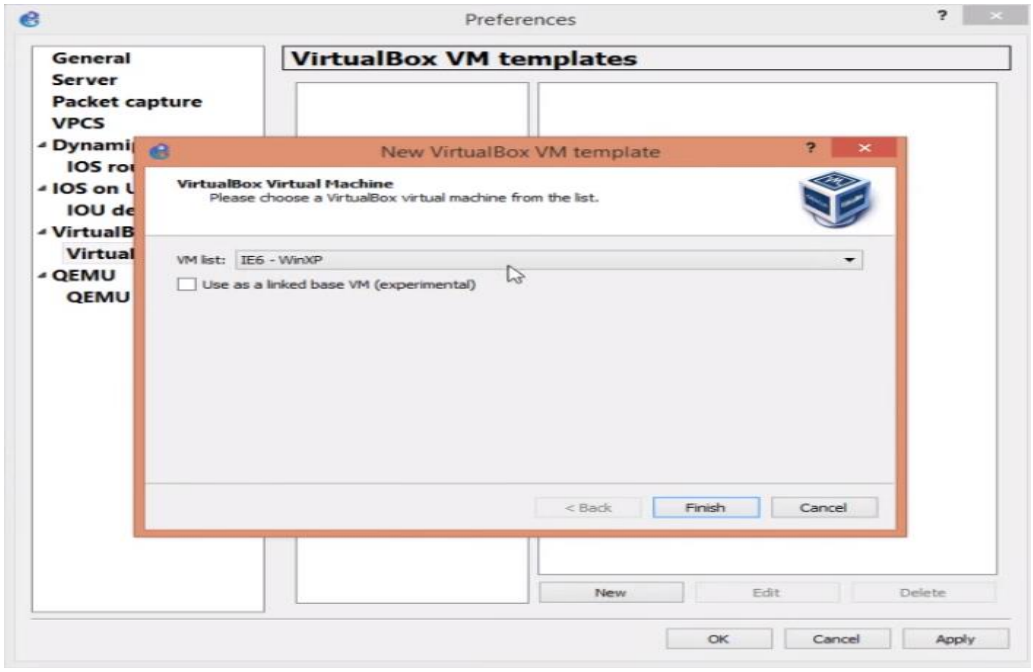

Рисунок 30 – Вікно вибору віртуальних машин

Далі перейдемо в налаштування, щойно доданої віртуальної машини та дозволимо GNS3 використовувати сконфігуровані VirtualBox адаптери. Після відмічання чекбоксу застосуємо зміни для GNS3 зроблені у вікні Preferences як на рисунку 31.

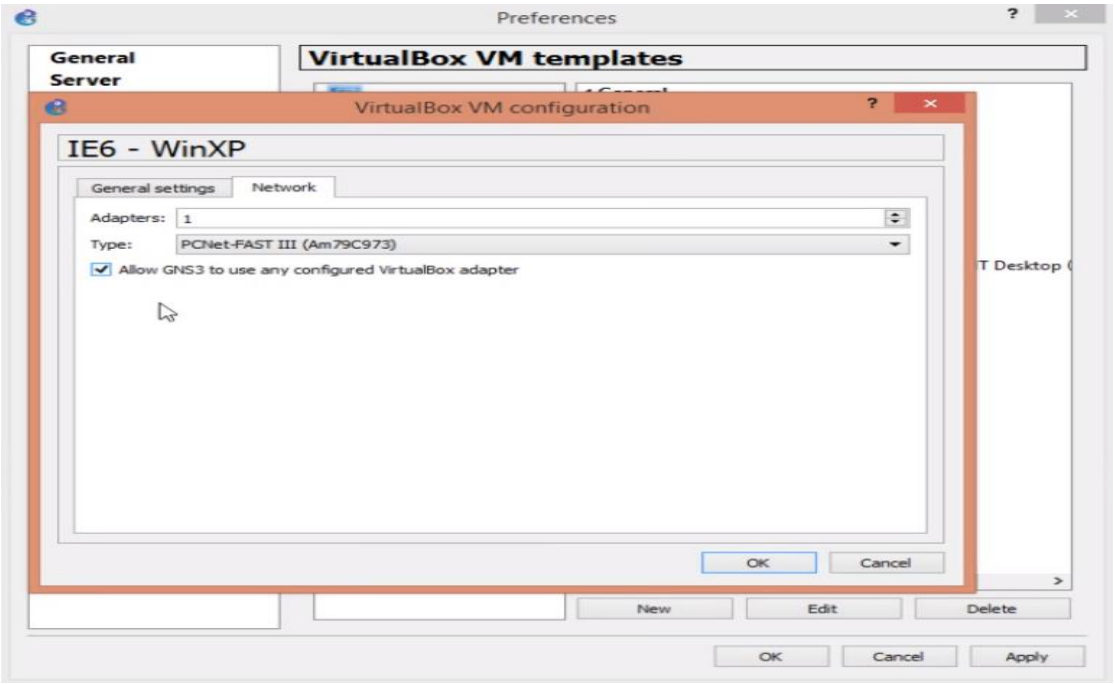

Рисунок 31 – Вікно налаштувань віртуальної машини

Далі перетягнемо іконку віртуальної машини на робочу поверхню імітаційної моделі. Натискаємо правої клавішею по віртуальній машині, з контекстного меню, як на рисунку 32, вибираємо Start (Запуск). Після чого з’явиться нове вікно віртуальної машини і наш хост з розгорнутою системою захисту буде запущено.

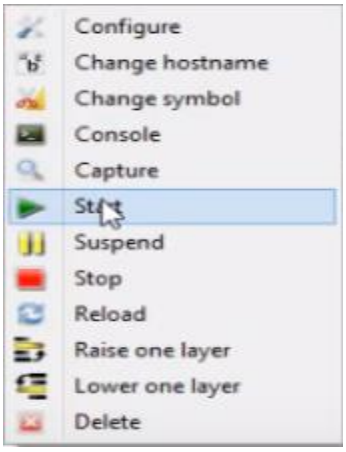

Рисунок 32 – Контекстне меню елемента на робочій поверхні GNS3

У вікні Consol (Консоль) як на рисунку 33 переконаємося, що підключений хост пінгується з даної мережі командою ping.

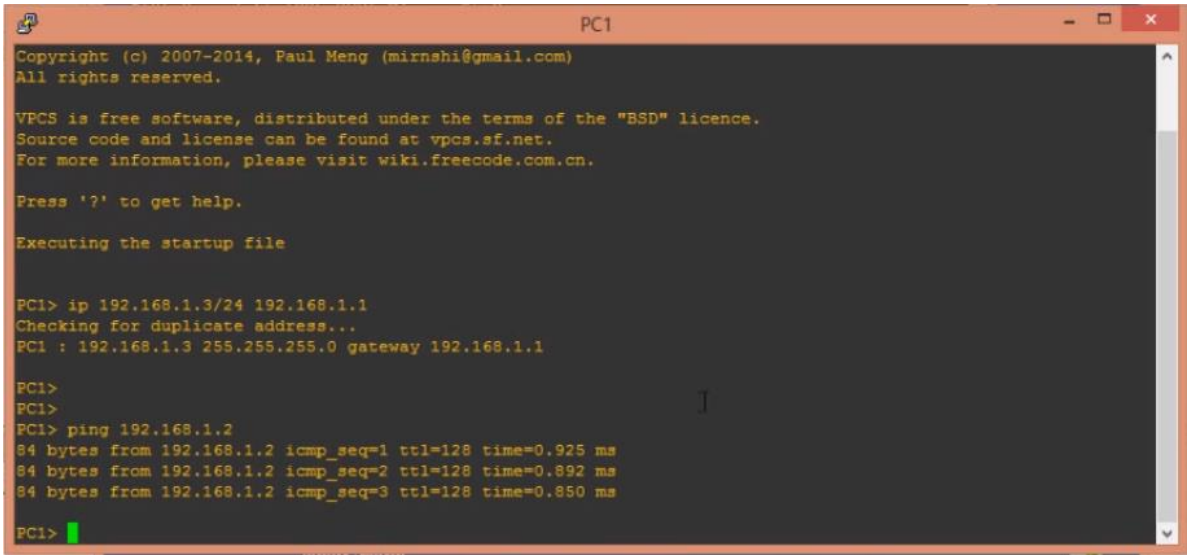

Рисунок 33 – Консольне вікно GNS3

Для другого хосту потрібно відтворити ідентичну послідовність дій. Після чого робоча поверхня в GNS3 буде мати наступний вигляд як на рисунку 34:

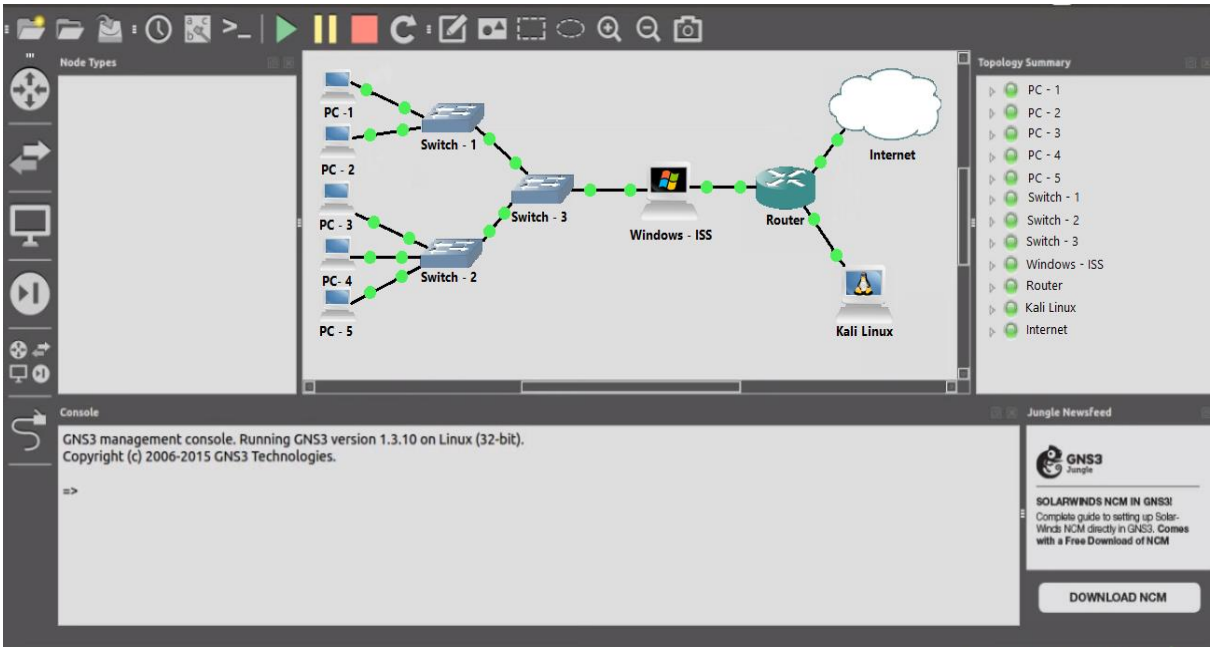

Рисунок 34 – Робоча поверхня GNS3 з налаштованою імітаційною мережею

Натиснемо кнопку старт для початку симуляції. Натиснемо правою клавішею на елемент топології Kali Linux. З контекстного меню виберемо пункт Start. У новому вікні знайдемо програму Vega. Почнемо атаку. У вікні вибору модулів як на рисунку 35 знімемо відмітки з усіх загроз окрім Cross-Site Scripting та SQL Injection.

Вибравши один з надісланих загрозливих запитів, можна розглянути детальну інформацію про згенерований запит та яку конкретно загрозу він містив у собі. На рисунку 36 наведено приклад вікна огляду загрозливого запиту, який був надісланий в корпоративну мережу.

Рисунок 35 – Вікно вибору модулів у Vega

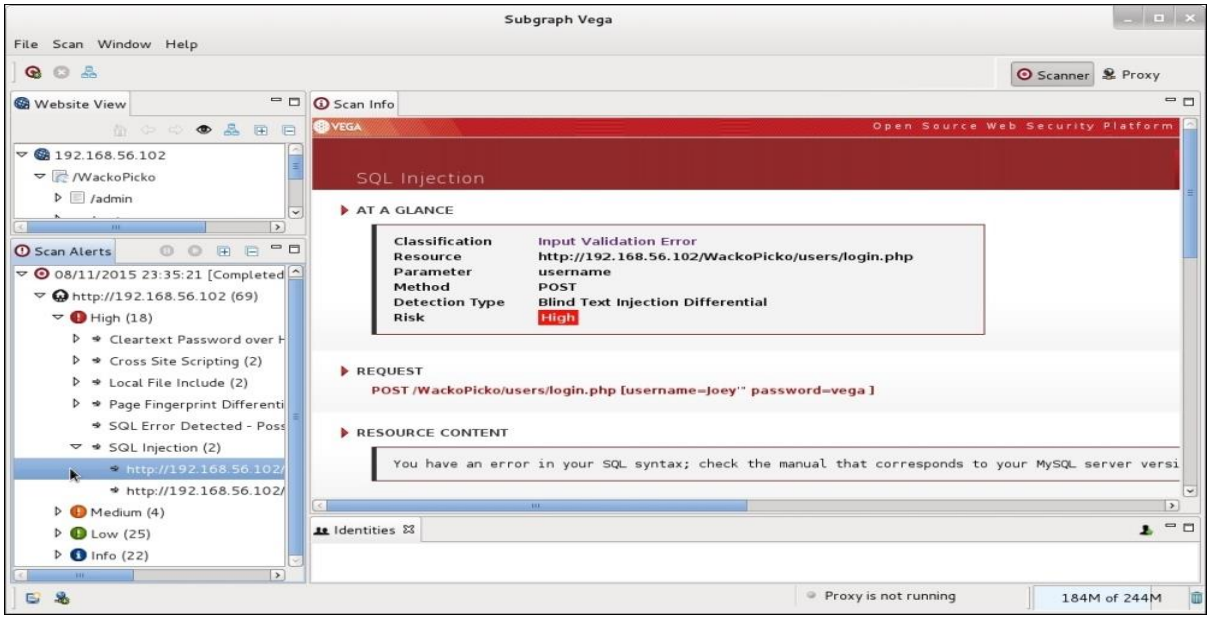

Рисунок 36 – Вікно огляду основної інформації про надісланий загрозливий запит

Відкривши віртуальну машину із запущеною системою захисту можна спостерігати за веденням логів на рисунку 38 та рисунку 39, яке відбувається за допомогою Logger мікросервісу.

На цьому симуляцію атак можна вважати завершеною. Далі розглянемо

статистичні дані приведені на рисунку 37 та рисунку 38, проведемо їх аналіз та зробимо висновки щодо ефективності розробленої системи захисту інформації в корпоративній мережі.

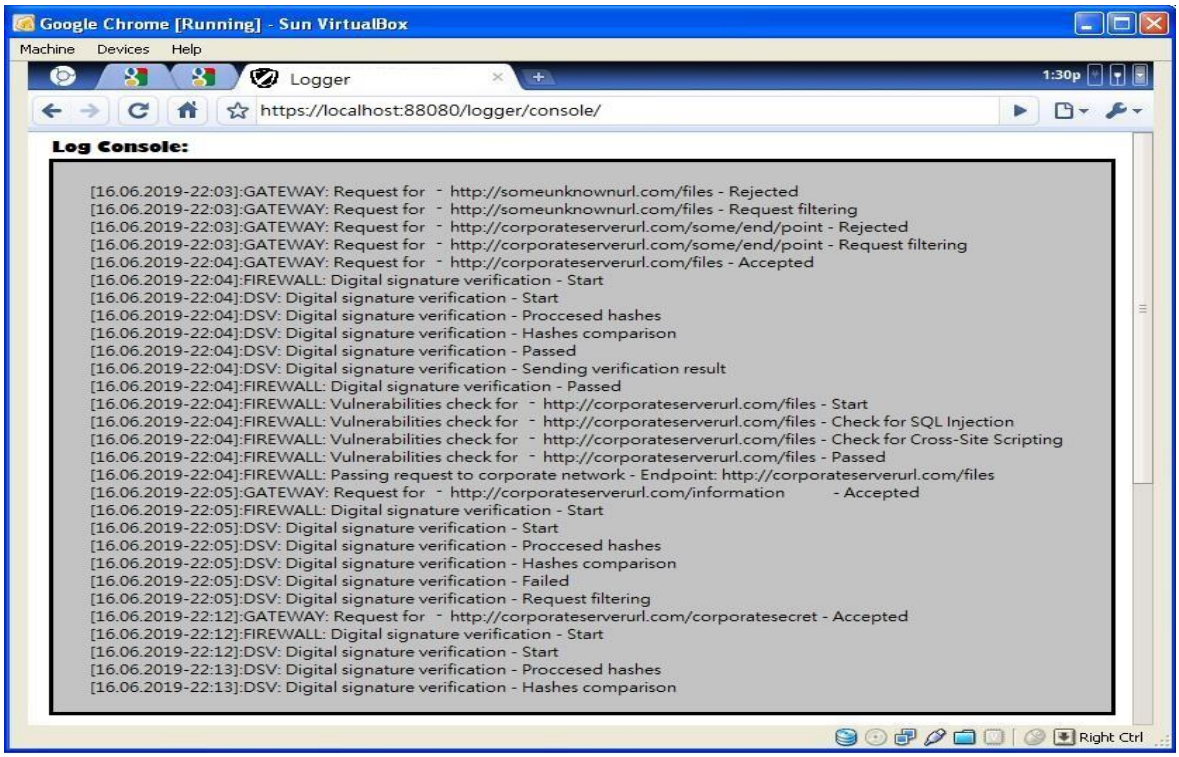

Рисунок 37 – Ведення логів у вікні мікросервіса Logger

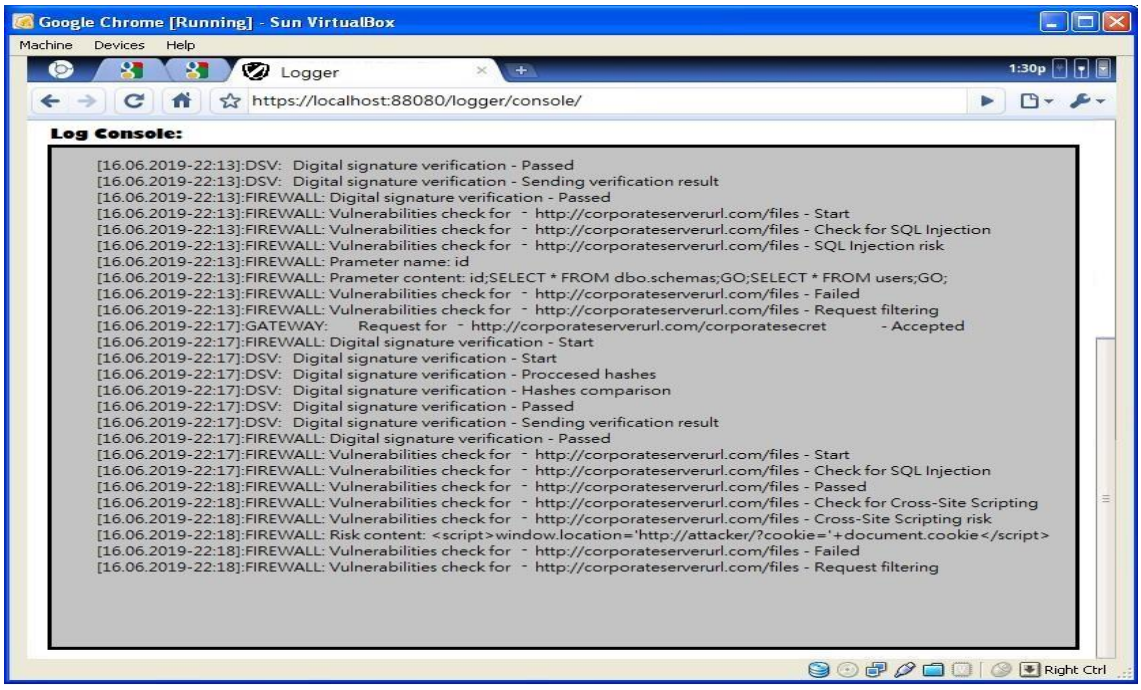

Рисунок 38 - Ведення логів у вікні мікросервіса Logger

ВИСНОВОКИ

У результаті виконанні дипломного проекту було розроблено легковбудовувану систему, яка складається зі спільно взаємодіючих мыж собою мікросервісів (Gateway, Firewall, DigitalSignatureVerifier та Logger), ціль якої забезпечити захист від одних з найбільш поширених веб-загроз, а саме SQL Injection та Cross-site scripting.

Так як основною технологією розробки був ASP.NET Core фреймворк, система може бути розгорнута на усіх операційних системах, які на даний момент підтримує ASP.NET Core (Windows, Linux, macOS). Винайдена система має аналоги тільки у вигляді часткових рішень. На разі готове рішення системи захисту, яка б включала в себе Firewall та Електронно-цифровий підпис тяжко знайти. А отже система легко знайде свого користувача. Система є повністю автономною. Після встановлення необхідних інструментарних додатків на розгортуваний комп'ютер або сервер система відкриває доступ тільки до Logger API. Дане API забезпечує доступ на сторінку ведення логів, на цій сторінці присутня повна звітність від моменту, коли веб-запит надійшов до Gateway, до моменту відправлення запиту до корпоративної мережі. Перевірка цифрового підпису забезпечує додатковий шар захисту і запобігає атакам, які відтворені в наслідок витоку інформації або витоку інформації за допомогою інсайдерів про endpoint-и корпоративної мережі. Запити, які влучили в один з зареєстрованих endpoint-ів і пройшли далі до Firewall-у будуть відсіяні на етапі перевірки цифрового підпису.

Проведені стрес тестування за допомогою програми Vega (Kali Linux) показують, що система надзвичайно стійка до атак типу XSS та SQL Injection. Розроблена система захисту має перспективи для подальшого ускладнення захисних механізмів або ж навіть вбудування додаткових шарів захисту наприклад, декілька ЕЦП, окремий мікросервіс для усунення та фільтрації загрозливих запитів будь якого типу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Infowatch: Главные каналы утечек информации [Електронний ресурс]: [Веб-сайт] Режим доступу: https://www.securitylab.ru/news/356791.php.
2. Утечки информации [Електронний ресурс]: [Веб-сайт] Режим доступу: https://www.anti-malware.ru/threats/leaks.
3. Robert M. Lee. Active Cyber Defense Cycle, 2016 – 651 с.
4. Lei Chen, Hassan Takabi, Nhien-An Le-KhacJohn Wiley & Sons. Security, Privacy, and Digital Forensics in the Cloud, 2019 – 360 с.
5. Glen D. Singh, Rishi Latchmepersad. CompTIA Network+ Certification Guide, 2018 – 422 с.
6. Dijiang Huang, Ankur Chowdhary, Sandeep Pisharody. Software-Defined Networking and Security: From Theory to Practice, 2018 – 328 с.
7. Kwangjo Kim, Muhamad Erza Aminanto, Harry Chandra Tanuwidjaja. Network Intrusion Detection Using Deep Learning: A Feature Learning Approach, 2018 – 79 с.
8. Webroot Business Endpoint Protection [Електронний ресурс]: [Веб-сайт] Режим доступу: https://www.webroot.com/us/en/business/smb/endpoint-protection-b.
9. Manage Engine Service Desk Plus [Електронний ресурс]: [Веб-сайт] Режим доступу: https://www.manageengine.com/products/service-desk.
10. What Is A Reverse Proxy? Proxy Servers Explained [Електронний ресурс]: [Веб-сайт] Режим доступу: https://www.cloudflare.com/learning/cdn/glossary/reverse-proxy/.
11. SQL Injection [Електронний ресурс]: [Веб-сайт] Режим доступу: https://docs.microsoft.com/en-us/sql/relational-databases/security/sql-injection?view=sql-server-2017.
12. Prevent Cross-Site Scripting (XSS) in ASP.NET Core [Електронний ресурс]: [Веб-сайт] Режим доступу:

https://docs.microsoft.com/en-us/aspnet/core/security/cross-site-scripting?view=aspnetcore-2.2.

13. Building a Reverse Proxy in .NET Core [Електронний ресурс]: [Веб-сайт] Режим доступу: https://auth0.com/blog/building-a-reverse-proxy-in-dot-net-core/.

14. Secure Azure Web sites with Web Application Gateway wtih end-to-end SSL connections [Електронний ресурс]: [Веб-сайт] Режим доступу: https://moimhossain.com/category/web-application-firewall/.